T-CY
CYBERCRIME CONVENTION COMMITTEE
COMITÉ DE LA CONVENTION CYBERCRIMINALITÉ

T-CY(2013)17rev
(provisoire)

Strasbourg, France
Version 3 décembre 2014

Rapport d'évaluation : Les dispositions de la Convention de Budapest sur la cybercriminalité concernant l'entraide

Adopté par le T-CY lors de sa 12ème Réunion Plénière (2-3 décembre 2014)

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Table des matières

1 Introduction 3

2 Évaluation de la fréquence des demandes d'entraide et les types de données stockées 5

2.1 Types de données demandées 5
2.2 Fréquence des demandes 6
2.3 Demandes d'entraide contre coopération policière 7
2.4 Information spontanée 9
2.5 Tableaux concernant les Questions 1.1 – 1.4 11

3 Évaluation des procédures et des conditions régissant l'entraide pour ce qui est de l'accès à des données stockées. 37

3.1 Conditions 37
3.2 Motifs de refus 39
3.3 Langue dans laquelle est formulée la demande 42
3.4 Procédure pour l'envoi/la réception des demandes 44
3.5 Problèmes rencontrés 45
3.6 Tableaux concernant les questions 2.1 – 2.5 47

4 Évaluation des canaux et moyens de coopération 95

4.1 Autorités, canaux et moyens de coopération 95
4.2 Demandes urgentes/réponses accélérées 97
4.3 Rôle des points de contact 24/7 98
4.4 Contact direct pour obtenir des données émanant de personnes physiques ou morales dans des juridictions étrangères 100
4.5 Coordination dans des affaires internationales complexes 100
4.6 Tableaux concernant les questions 3.1 – 3.4** 102

5 Conclusions et recommandations 136

5.1 Conclusions 136
5.2 Recommandations 139
5.3 Suites à donner 141

6 Annexes 142

6.1 Liste des solutions proposées pour prendre l'entraide plus efficiente 142
6.2 Compilation de législations nationales pertinentes 148
6.3 Extraits de la Convention de Budapest sur la cybercriminalité 213

Contact

Alexander Seger
Secrétaire du Comité de la Convention sur la cybercriminalité (T-CY)
Direction Générale Droits de l'homme et État de droit
Conseil de l'Europe, Strasbourg, France

Tél +33-3-9021-4506
Fax +33-3-9021-5650
Email : alexander.seger@coe.int

1 Introduction

Une entraide judiciaire rapide est l'une des conditions les plus importantes pour obtenir des mesures efficaces contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques, étant donné la nature transnationale et volatile de ces dernières. En pratique, cependant, les procédures pour l'entraide judiciaire sont considérées trop complexes, prenant trop de temps et mobilisant trop de ressources, et donc trop inefficientes.

Le Comité de la Convention sur la cybercriminalité (T-CY), lors de sa 8e Session plénière (5-6 décembre 2012), a donc décidé d'évaluer en 2013 l'efficience de certaines dispositions du Chapitre III de la Convention de Budapest sur la cybercriminalité relatives à la coopération internationale. Lors de sa 10e Plénière (2-3 décembre 2013), il a décidé de prolonger cette évaluation en 2014.

La Convention de Budapest sur la cybercriminalité est un traité de justice pénale. Le Chapitre III sur la coopération internationale fait référence à la coopération « aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. »[1].

Le T-CY a décidé de concentrer l'évaluation en particulier sur l'article 31, qui prévoit « l'entraide concernant l'accès aux données stockées » selon une procédure accélérée :

> Article 31 – Entraide concernant l'accès aux données stockées
>
> 1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.
>
> …
>
> 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
>
> a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou
>
> b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

La présente évaluation a pour but d'identifier des solutions permettant une entraide plus «rapide» afin de rendre la coopération internationale en générale plus efficiente.

L'article 31 est évalué dans le contexte du régime plus large de coopération internationale, autrement dit en relation avec les articles 23, 25, 26, 27, 28 et 35 de la Convention de Budapest.

Un questionnaire préparé par le Bureau du T-CY a été diffusé aux Parties et Observateurs le 18 février 2013 pour réponse au plus tard le 10 avril 2013. La 9e Plénière du T-CY (4-5 juin 2013) a tenu un premier cycle de discussions sur la base de la compilation des réponses reçues (voir tableau des réponses reçues), un deuxième cycle lors de la 10e Plénière les 2-3 décembre 2013 et un troisième cycle lors de la 11e Plénière les 17-18 juin. Des réponses ou commentaires additionnelles ont été reçues suites aux discussions lors de ces Plénières. Le présent rapport a été adopté par la 12e Plénière du t-CY (2-3 décembre 2014).

---

[1] Voir Articles 23 et 25.1 Convention sur la cybercriminalité.

Le rapport est basé sur les réponses reçues au questionnaire et autres commentaires et contributions reçus entre avril 2013 et novembre 2014 des Etats suivants :

1. Albanie
2. Arménie
3. Australie
4. Autriche
5. Azerbaïdjan
6. Belgique
7. Bosnie-Herzégovine
8. Bulgarie
9. Costa Rica
10. Croatie
11. Chypre
12. Danemark
13. République dominicaine
14. Estonie
15. Finlande
16. France
17. Géorgie
18. Allemagne
19. Hongrie
20. Islande
21. Italie
22. Japon
23. Lettonie
24. Lituanie
25. Malte
26. Maurice
27. République de Moldova
28. Monténégro
29. Pays-Bas
30. Norvège
31. Portugal
32. Roumanie
33. Serbie
34. Slovaquie
35. Slovénie
36. Espagne
37. Suisse
38. «l'ex-République yougoslave de Macédoine»
39. Turquie
40. Ukraine
41. Royaume-Uni
42. États-Unis d'Amérique

2 Évaluation de la fréquence des demandes d'entraide et les types de données stockées

2.1 Types de données demandées

Dans le cadre de la coopération internationale, les types d'information suivants sont demandés aux autorités étrangères :

- les informations sur les abonnés[2] ressortent de la plupart des réponses comme constituant le type de données le plus fréquemment recherché. Cette catégorie recouvre les informations permettant d'identifier l'utilisateur d'une adresse IP (ou, a contrario, des informations sur l'adresse IP utilisée par une personne donnée) ou le propriétaire d'un compte de messagerie électronique, sur des réseaux sociaux ou VOIP ainsi que des informations techniques connexes liées à la localisation, à l'équipement utilisé etc. Les requêtes visent souvent des informations sur les moyens de paiement ou des données de facturation.

- Cette catégorie est suivie par les demandes concernant des données relatives au trafic, en particulier les fichiers journaux d'IP ou de téléphones portables.

- Les données relatives au contenu semblent faire moins fréquemment l'objet de demandes d'entraide et, lorsqu'elles sont demandées, elles concernent le contenu de courriers électroniques, de comptes sur des réseaux sociaux et de messages sur des forums de discussion ou similaire, ou encore des contenus illégaux tels que du matériel pédopornographique.

Pour ce qui est des infractions principales :

- la presque totalité des réponses mentionnent la fraude et d'autres délits financiers sous toutes leurs formes, depuis la fraude aux cartes de crédit jusqu'à la fraude au paiement en ligne en passant par la fraude aux enchères, le hameçonnage et d'autres types de faux informatiques et de fraude liée à des infractions traditionnelles telles que l'abus de confiance, la corruption, l'évasion fiscale, le blanchiment d'argent et des infractions similaires.

- Les crimes violents et crimes graves constituent des infractions motivant des demandes d'obtention de données dans de nombreux États. Cette catégorie peut couvrir le meurtre, les agressions, le trafic d'êtres humains, le trafic de stupéfiants, le blanchiment d'argent, le terrorisme et son financement, l'extorsion et, en particulier, la pédopornographie et autres formes d'exploitation et d'abus sexuels à l'encontre des enfants.

---

[2] Définition de l'article 18(3) de la Convention de Budapest :
Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:
a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

- De nombreuses réponses citent également les infractions à l'encontre de systèmes informatiques (accès illégal, interception illégale, diffusion de logiciels malveillants, interférence avec des données).

- Un petit nombre de pays évoquent la diffamation et la calomnie (Philippines, Portugal, Slovaquie, Turquie), la xénophobie et les discours de haine (Bosnie-Herzégovine, Serbie), les violations du droit de la propriété (Moldova) ou les jeux en ligne (Malte).

Conclusions préliminaires :

- L'entraide judiciaire pour accéder à des données stockées ne concerne pas seulement les infractions à l'encontre ou par des ordinateurs (Articles 2 à 11 Convention de Budapest), mais couvre la collecte de preuves sous forme électronique liées à toute infraction pénale (comme prévu à l'article 23 Convention de Budapest). Cette large portée est conforme aux dispositions de l'article 14.

- D'un autre côté, les pouvoirs et procédures au niveau national doivent être établis « aux fins d'enquêtes ou de procédures pénales spécifiques, ce qui restreint l'application des mesures à une enquête concernant une affaire donnée »[3]. Cette limitation à des enquêtes criminelles spécifiques ou à des données ou communications spécifiées s'applique également aux dispositions relatives à la coopération internationale.

2.2 Fréquence des demandes

La plupart des pays n'ont pas été en mesure de communiquer des statistiques sur la fréquence des demandes d'entraide en vue d'accéder à des données stockées sur informatique. Plusieurs raisons semblent expliquer cette impossibilité :

- l'entraide judiciaire est de plus en plus décentralisée et les demandes sont envoyées ou reçues directement au niveau des autorités judiciaires et pas uniquement via les autorités centrales. En général, ces dernières n'exécutent pas les demandes elles-mêmes. L'envoi ou la réception de demandes, et en particulier leur exécution, peut impliquer plusieurs services.

- Les demandes pour des preuves électroniques ne font pas l'objet d'une collecte distincte de statistiques.

Les données statistiques disponibles étant limitées, il est difficile de faire une analyse. Les données ci-dessous en sont un bon exemple :

État	**Demandes reçues pour l'obtention de données**	**Demandes envoyées pour l'obtention de données**
Albanie	8 (2012)	environ 12 (2012)
Australie	10 (2011/12)	97 (2011/12)
Japon	11 (2013	1 (2013)
Lituanie	4-5 par an	3-4 par an
République de Moldova	27 (2013)	15 (2013)
Norvège	37 (2012)	n/d

[3] Paragraphe 152 Rapport explicatif.

Roumanie[4]	95 (2012)	284 (2012)
Serbie[5]		55 (2008-May 2014)
Turquie	11 (2012)	364 (2012)
États-Unis	Des centaines de demandes	Des centaines de demandes

Les réponses semblent suggérer que l'entraide est considérée comme trop complexe et mobilisant trop de temps et de ressources pour l'obtention de preuves électroniques, et qu'en conséquence, il est fréquent qu'elle ne soit pas utilisée. Les services répressifs tendent à obtenir des informations par le biais de la coopération policière pour éviter l'entraide, même si les informations ainsi obtenues ne peuvent la plupart du temps pas être utilisées dans les poursuites pénales. Fréquemment, les autorités contactent directement des fournisseurs de services à l'étranger (en particulier ceux qui sont basés aux États-Unis) pour obtenir des données relatives aux abonnés ou au trafic[6]. Souvent, les enquêtes sont abandonnées.

2.3 Demandes d'entraide contre coopération policière

La coopération entre services de police pour le partage de données sur la cybercriminalité et constituant des preuves électroniques est beaucoup plus fréquente que l'entraide (le ratio semble aller de 10 pour 1 à 50 pour 1).

De manière générale, il ressort que :

- la coopération policière vise à échanger des renseignements qui pourraient déboucher sur le déclenchement de procédures judiciaires pénales ;
- les informations obtenues par le biais de la coopération policière ne peuvent souvent pas être utilisés dans les procédures judiciaires pénales ;
- l'entraide a pour but d'obtenir des preuves qui seront utilisées dans des poursuites pénales (poursuites et procédures judiciaires) ;
- dans certaines Parties, seul le matériel reçu par le biais l'entraide judiciaire peut être utilisé en tant que preuve devant un tribunal (par exemple, en Australie). D'autres se réfèrent au principe de l'appréciation libre de la preuve devant les tribunaux (Finlande, Hongrie, Slovaquie) et dans d'autres, cela dépend du cas en question (Allemagne[7], Serbie[8]) ;

[4] Statistiques fournies par la Directions pour les enquêtes en matière de crime organisée et de terrorisme par le Ministère Public attaché à la Haute Cour de Cassation et de Justice. Les statistiques comprennent des demandes faites durant la phase d'enquête.

[5] Statistiques du Bureau special du procureur pour les crime High-Tech seulement

[6] Voir rapports de transparence sur les demandes des services répressifs à différentes sociétés sur le site http ://www.google.com/transparencyreport/?hl=en-GB

[7] Commentaire de l'Allemagne : l'utilisation au tribunal d'informations obtenues par la coopération policière, conformément à la décision-cadre 2006/960 de l'UE, l'utilisation de ces informations est restreinte au but pour lequel elles ont été transmises à l'origine. Pour être utilisées comme preuves au tribunal, il faut l'accord supplémentaire de l'État qui les a transmises.

[8] Commentaire de la Serbie : les informations recueillies par le biais d'une coopération policière ne doivent être utilisées qu'aux fins de l'enquête et non comme preuves dans des procédures judiciaires ; toutefois, elles peuvent servir de preuves dès lors qu'elles sont considérées comme admissibles par le droit interne serbe.

- pour des informations exigeant des mesures coercitives au niveau national – et donc une injonction du tribunal -, une demande formelle d'entraide est nécessaire ;

- pour les données relatives au contenu, et en principe également pour celles qui concernent le trafic, une demande formelle d'entraide est requise. En attendant son activation, il conviendrait de faire une requête de conservation au titre des articles 29 ou 30 afin de conserver les données.

Pour ce qui est des données qui peuvent être partagées sans demande d'entraide, la situation semble plus contrastée en fonction des États répondants :

- l'Arménie peut fournir des données relatives au trafic sans demande d'entraide mais à condition de recevoir une demande officielle décrivant l'affaire et les informations demandées. Si nécessaire, une injonction peut être obtenue en Arménie ;

- l'Australie peut communiquer à des services répressifs étrangers, à des fins d'enquête, des données spécifiées relatives au trafic ou à l'abonné sur la base d'une coopération policière.

- L'Allemagne (sous condition de réciprocité), la Hongrie, la Suisse, la Turquie peuvent partager des informations concernant l'abonné sans demande d'entraide.

- Les Philippines peuvent partager des preuves d'activités illégales commises par des ressortissants étrangers.

- Les données pouvant être obtenues au niveau national par la police sans mesures contraignantes, et donc sans injonction judiciaire, peuvent être partagées (par l'Australie[9], la Belgique, Chypre, la Finlande[10], la France, le Japon[11], la Serbie, la Suisse).

- Des données obtenues dans des affaires nationales ou des données opérationnelles déjà connues de la police peuvent être partagées (par l'Albanie, la Belgique, la Bosnie-Herzégovine, la Lettonie, la Lituanie, la Norvège, le Portugal, la Roumanie, la Slovénie, les États-Unis).

- Les données ne concernant pas le contenu peuvent être obtenues directement par l'autre pays avec l'accord du fournisseur (États-Unis).

Conclusions préliminaires :

- L'ouverture d'une enquête au niveau national après une demande étrangère ou un échange spontané d'information devrait faciliter le partage des informations sans demande d'entraide ou accélérerait le traitement de la demande d'entraide.

- Dans des enquêtes communes, des preuves peuvent être recueillies ou se trouver imbriquées dans des preuves de nature nationale mais être partagées de manière informelle durant l'enquête.

---

[9] Les données peuvent être obtenues au niveau national par la police sans mesures obligatoires et donc sans ordonnance du Tribunal peuvent être partagés dans certaines circonstances pour l'Australie : le matériel obtenu volontairement par la police pour un seul but ne peut être utilisé pour une autre fin qu'avec consentement.

[10] Observation de la Finlande : toutes les demandes d'entraide dans la phase d'enquête criminelle sont couvertes par la législation et les procédures finlandaises en matière d'entraide. La question de l'autorité compétente pour exécuter l'entraide est une question différente.

[11] Observation du Japon : ces données ne peuvent être utilisées comme preuve devant la justice.

Dans ce cas, cette mise en commun pourrait être formalisée ultérieurement si nécessaire aux fins de procédures pénales.

- La distinction entre coopération policière et demande d'entraide n'est pas toujours très claire. Ceci est également vrai concernant l'admissibilité de la preuve devant les tribunaux du matériel reçu dans la cadre de la coopération policière.

- Dans certains pays, une différenciation supplémentaire peut être nécessaire entre les demandes d'entraide au stade de l'enquête et la coopération entre tribunaux. Au stade des tribunaux, la preuve exiger la coopération par le biais de ministères de la Justice ou la coopération de tribunaux à tribunaux, tandis que d'autres solutions peuvent être possible pendant la phase d'enquête.

2.4 Information spontanée

La transmission d'informations spontanée est prévue à l'article 26 de la Convention de Budapest :

> Article 26 – Information spontanée
>
> 1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.
>
> 2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Il ressort des réponses que les États appréhendent et utilisent tout à fait différemment cette possibilité :

- jamais ou rarement utilisée, ou aucune expérience: Estonie, France, Hongrie, Japon, Lituanie, Malte, Pays-Bas, Slovaquie, Slovénie, Espagne, et «ex-République yougoslave de Macédoine».

- pas très souvent : Albanie, Arménie, Bosnie-Herzégovine, Géorgie, Roumanie, Slovaquie.

- souvent/très souvent : Chypre (envois : 50/an, réceptions : 35/an), Allemagne (quotidiennement), Lettonie, Philippines, Portugal, Serbie, Suisse (envois : 5-10/semaine, réception: 1/mois), Turquie, Ukraine, États-Unis (en permanence).

Avantages :

- la transmission spontanée d'informations déclenche des enquêtes au niveau national dans le pays qui les reçoit (Albanie, Autriche, Belgique, Bosnie-Herzégovine, Bulgarie, Costa Rica, Croatie, Norvège, Portugal et États-Unis).

- Cela peut aboutir à des opérations impliquant plusieurs pays (République dominicaine).

- Cela peut aboutir à des demandes d'entraide (Croatie).

- Cela peut servir pour une coopération directe entre services (Australie).

- Les informations peuvent être partagées par le biais des officiers de liaisons dans les services répressifs étrangers (Philippines).

- Cela atténue le besoin de passer par des demandes d'entraide (États-Unis).

- La transmission spontanée d'informations concernant des adresses IP infectées permet ensuite aux services répressifs de contacter les fournisseurs de services qui informeront alors leurs clients (France).

- Précieuses informations pour l'analyse et les enquêtes concernant des schémas criminels organisés complexes (Chypre, Géorgie, Philippines, Suisse).

- Utile en situation d'extrême urgence avec risque de mort par exemple (Turquie).

Conclusion préliminaire :

- L'article 26 de la Convention de Budapest semble insuffisamment utilisé. Ceux qui échangent des informations semblent passer par d'autres accords soit sont autorisés par leur propre droit à agir sans référence à un accord.

2.5 Tableaux concernant les Questions 1.1 – 1.4

2.5.1 Informations demandées (Question 1.1) et infractions connexes (Question 1.2)

1.1 Types de données stockées généralement demandées par la voie de l'entraide (par exemple renseignements sur l'abonné, données relatives au trafic, données relatives au contenu)

Sur quel type de données stockées portent généralement les demandes que vous recevez ? Selon quelle fréquence ? Veuillez donner, si possible, des statistiques sur la fréquence/quantité de demandes.

Sur quel type de données stockées portent généralement les demandes que vous adressez à d'autres pays ? Selon quelle fréquence ? Veuillez donner, si possible, des statistiques sur la fréquence/quantité de demandes.

1.2 Types d'infractions pour lesquelles des données stockées sont généralement demandées par la voie de l'entraide (veuillez donner des statistiques si possible)

À quel type d'infractions sont généralement liées les demandes que vous recevez concernant des données stockées ? Veuillez donner des exemples.

Lorsque vous adressez à d'autres Parties des demandes concernant des données stockées, sur quelles infractions ces demandes portent-elles généralement ? Veuillez donner des exemples.

Pays	**Demandes entrantes**		**Demandes sortantes**	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
Albanie	Informations sur l'abonné uniquement (en particulier journaux IP). *Fréquence* : 6 demandes cette année, 8 demandes l'an dernier.	Infractions de fraude liées à l'informatique	Informations sur l'abonné uniquement. *Fréquence* : ≤ 1 demande/mois.	Cyber-délits. Autres : fraude, contrefaçon et délits aux cartes de paiement)
Arménie	Données relatives au trafic. Peu de demandes par an.	- Fraudes et faux liés à l'informatique - Diffusion de matériel	Environ 50 demandes/an : - Fichiers journaux - Informations sur le compte	- Fraudes et faux liés à l'informatique - Diffusion de matériel pornographique, y compris pédopornographique

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
		pornographique, y compris pédopornographique - Fraude aux cartes de crédit et paiements électroniques - Contenu illégal - Chantage (via Internet) - Dissémination de logiciels ou programmes malveillants - Accès illégal à un système ou réseau informatique - Possession illégale d'informations informatiques	d'un utilisateur de réseaux sociaux (pas le contenu) - information clients pour certains utilisateurs d'adresses IP. - Informations relatives à des paiements électroniques.	- Fraude aux cartes de crédit et paiements électroniques - Contenu illégal - Chantage (via Internet) - Dissémination de logiciels ou programmes malveillants - Accès illégal à un système ou réseau informatique - Possession illégale d'informations informatiques
Australie	Informations FSI, Renseignements concernant des abonnés et contenu stocké. *Fréquence* : 10 demandes en un an (2011-2012)	Essentiellement fraude. Autres : corruption à l'étranger, meurtre, association de malfaiteurs et infractions à la législation sur les stupéfiants	Informations FSI, Renseignements concernant des abonnés et du contenu stocké. *Fréquence* : 97 demandes en un an (2011-2012)	Essentiellement infractions concernant les stupéfiants et délits sexuels sur enfants. Autres : corruption à l'étranger, meurtre, agression, vol, immigration et trafic de clandestins.
Autriche	Pas de statistiques. L'autorité centrale traite tous types de données.	Pas de statistiques. Fraudes et autres formes de délits financiers. Rarement : extorsion ou kidnapping.	Pas de statistiques. L'autorité centrale traite tous types de données.	Similaires aux infractions concernant les demandes entrantes.
Azerbaïdjan			Renseignements concernant des abonnés (Adresse IP). Quelques demandes par les points de contact 24/7	Des attaques cyber sur le sinfrastructures critiques et piratage.
Belgique	Principalement des renseignements concernant des abonnés et des	En général, demandes pour des données stockées liées au terrorisme ou au financement	Principalement des renseignements concernant des abonnés et des données sur	Demandes concernant principalement des données aux États-Unis pour le même type d'infraction (terrorisme ou

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
	historiques de connexion de l'IP	du terrorisme, aux délits financiers notamment le blanchiment d'argent, et à la fraude, notamment abus de confiance	l'historique de connexion IP.	financement du terrorisme, délits financiers notamment blanchiment d'argent, et fraude, notamment abus de confiance).
Bosnie-Herzégovine	Renseignements concernant des abonnés essentiellement (Adresse IP). *Fréquence :* peu de demandes d'entraides par an ; peu de demandes par les points de contact 24/7.	Accès non autorisé à un système/système protégé de traitement de données électronique, fraude informatique.	Renseignements concernant des abonnés (Adresse IP). *Fréquence* : ≈ 1 demande/mois.	Blanchiment d'argent, fraude fiscale, terrorisme, incitation à la haine nationale, raciale et religieuse, à la discorde et à l'hostilité, usage illicite du droit de diffusion. District de Brčko : menaces à la sécurité, corruption, délits liés à un système de traitement de données électroniques.
Bulgarie	Tous types de données (pas de statistiques fournies).	Essentiellement fraude financière, bancaire et fiscale, blanchiment d'argent, hameçonnage et pédopornographie.	Typiquement des renseignements concernant des abonnés et des données relatives au trafic, informations financières.	Essentiellement fraude financière, bancaire et fiscale, blanchiment d'argent, hameçonnage et pédopornographie.
Costa Rica	Dépend du type d'enquête et des infractions objet de l'enquête.	Dépend de l'affaire en cause et du délit objet de l'enquête.	Dépend de l'affaire en cause et du délit objet de l'enquête (par exemple, pour le délit de pédopornographie : images, vidéos, adresses IP, etc.)	Impossible d'établir une liste précise. Exemples possibles : pédopornographie, faux informatiques ou fraude liée à l'informatique, et menaces à l'aide de services ou dispositifs électroniques.
Croatie	Pas de données	Pas de données	Pas de données	Pas de données
Chypre	30 demandes par an : - Info sur abonnés d'adresses IP - Fichiers téléchargés - Info connexions - Info sites web	- Piratages - Fraude	20 demandes par an sur : - Info sur abonnés d'adresses IP - Fichiers téléchargés - Info connexions - Info sites web	- Piratages - Affaires de pédopornographie

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
République dominicaine	N/A	N/A	Données pour identifier des utilisateurs ou abonnés de comptes de messagerie électronique ou d'adresses IP.	N/A
Estonie	Pas d'informations.	Pas d'informations.	Pas d'informations.	Pas d'informations.
Finlande	Pas de statistiques. Essentiellement des renseignements concernant des abonnés, des données relatives au trafic et relatives au contenu.	Différents types de délits : cyber-délits, ainsi que des homicides, violences à enfants et délits financiers.	Pas de statistiques. Essentiellement des renseignements concernant des abonnés, des données relatives au trafic et relatives au contenu.	Différents types de délits : cyber-délits, ainsi que des homicides, violences à enfants et délits financiers.
France	Pas de statistiques. Renseignements concernant des abonnés, données relatives au trafic, adresses de messagerie électronique, dossiers judiciaires, dossiers administratifs, etc.	Délits liés au traitement automatique de données, fraude sur Internet, fraude aux cartes de crédit	Pas de statistiques. Renseignements concernant des abonnés, données relatives au trafic, adresses de messagerie électronique, dossiers judiciaires, dossiers administratifs, etc.	Délits liés au traitement automatique de données, fraude sur Internet, fraude aux cartes de crédit.
Géorgie	Pas de statistiques.	Pas de statistiques.	Pas d'exemples.	Pas d'exemples.
Allemagne	Pas de statistiques. Essentiellement des images informatiques forensiques.	Fraude, piratage/sabotage informatique.	Pas de statistiques. Essentiellement données sur l'abonné, sur le trafic et sur le contenu à partir de comptes de messagerie électronique et de réseaux sociaux.	Tous types d'infraction. Fréquemment homicide, fraude, pédopornographie et violences sur enfants.
Hongrie	Données sur l'abonné Données de trafic relatives aux appels	Atteinte aux biens Crime violent	Données sur l'abonné Données de trafic relatives aux appels	
Islande	Essentiellement des données sur l'abonné (sevices d'hébérgement Web,	Typiquement fraude liée à l'informatique, délits économiques, fraude, intrusions	Essentiellement données relatives aux abonnés (sevices d'hébérgement Web).	Essentiellement des menaces, trafic de stupéfiants, fraude informatique et violence sexuelle.

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
	vérification d'adresses IP	informatiques	Approximativement 2-3/an	
Italie	n/a.	Piratage, fraude sur Internet, pédopornographie	n/a.	Cyber-attaques contre des infrastructures critiques, piratage, fraude sur Internet.
Japon	Renseignements concernant des abonnés, données relatives au trafic, adresses IP, contenu de messagerie électronique. *Fréquence* : une fois par an environ.	Accès illégal à des systèmes informatiques ; pédopornographie.	Renseignements concernant des abonnés, données relatives au trafic. *Fréquence* : pas de statistiques.	Fraude bancaire ou à la consommation en ligne, création de site web pour le hameçonnage, pédopornographie.
Lettonie	Essentiellement données relatives au contenu. *Fréquence* : deux demandes par mois en moyenne.	Typiquement fraude liée à l'informatique et accès illégal à un système informatique par exemple utilisation d'un service d'hébergement de page web dans le pays pour faire des ventes fictives.	Essentiellement données relatives au trafic et données relatives au contenu. *Fréquence* : une demande par mois en moyenne.	Interception illégale, fraude et accès illégal liés à l'informatique, par exemple utilisation d'un compte de messagerie électronique pour communiquer avec un FSI, une victime ou un complice de fraude aux cartes de crédit.
Lituanie	Renseignements concernant des abonnés, données relatives au trafic, copies forensiques de disques durs d'un PC ou de données de serveurs. *Fréquence* : 4-5 demandes par an.	Pas d'informations disponibles.	Renseignements concernant des abonnés, des données relatives au trafic ainsi que des données relatives au contenu. Par exemple affaires de pédopornographie : adresses IP, copies de fichiers journaux, messages de discussions sur Gmail, etc. *Fréquence* : 3-4 demandes par an.	Escroquerie, interception et utilisation illégales de donnée électroniques, connexion illégale à un système d'information etc. Par exemple affaire concernant l'introduction illégale d'un code malveillant dans des systèmes informatiques connectés à des comptes bancaires électroniques, contrôlés par un serveur en Allemagne. *(Voir réponse détaillée pour plus d'informations)*

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
Malte	Renseignements concernant des abonnés et données relatives au trafic (VOIP, paiements en ligne, sites web de jeux)	Les demandes sont souvent en lien avec des casinos en ligne afin de saisir des informations détenues par des sociétés de jeu en ligne.	Renseignements concernant des abonnés et données relatives au trafic couvrant des informations sur l'utilisateur fournies lors de l'enregistrement, comptes en lignes associés, informations sur les paiements et informations techniques (adresse IP, date, horodatage et fuseau horaire), contenu d'une boîte de messagerie en cas de crime grave	
Moldova	Données sur l'abonné (nom, adresse, messagerie électronique, etc.) ; données relatives au trafic (fichiers journaux).	Violation du droit de la propriété, pédopornographie, accès illégal à des données informatiques, interception illégale, fraude, etc.	Données sur l'abonné (nom, adresse, messagerie électronique, etc.) ; données relatives au trafic (fichiers journaux).	Violation du droit à la vie privée, violations du droit de la propriété, pédopornographie, accès illégal et autres cyber-délits, fraude, etc.
Monténégro	Pas de demandes jusqu'ici. Renseignements concernant des abonnés (adresse IP) [à clarifier]	Infractions en lien avec la pédopornographie, accès non autorisé à une base de données protégée.	Pas de demandes jusqu'ici. Renseignements concernant des abonnés (adresse IP) [à clarifier]	n/a.
Pays-Bas	Pas de données disponibles.	Pas de données disponibles.	Pas de données disponibles.	Pas de données disponibles.
Norvège	Essentiellement renseignements concernant des abonnés, journaux IP (services d'hébergement web et autres), et journaux d'appareils cellulaires ; données relatives au contenu	Pas de données sur les connexions IP provenant de FSI. Fraude et autres délits financiers (12 demandes sur 37), menaces et harcèlement (10), images de violences à	Pas de statistiques sur les demandes sortantes. Essentiellement renseignements concernant des abonnés, journaux IP (Facebook, Skype, services d'hébergement web), journaux de téléphones	Meurtre, crimes graves liés aux stupéfiants, vols avec violence, agressions sexuelles aggravées. Autres : délits informatiques, infractions graves, fraudes etc. *Fréquence* : pas de statistiques nationales.

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
	aussi. *Fréquence* : 37 demandes en 2012 (hors journaux de téléphonie et connexes)	enfants (5), intrusions informatiques (3) et autres délits (meurtres, délits liés aux stupéfiants etc.).	cellulaires ; données relatives au contenu aussi.	
Philippines	Vérifications d'adresse IP et renseignements concernant des abonnés. Demandes rares.	Piratage, violation de la loi sur l'accès aux dispositifs et pédopornographie.	Détails concernant les comptes Facebook, de messagerie électronique ou similaires. Demandes fréquentes.	Pédopornographie, violence à l'égard des femmes, abus à l'égard d'enfants et calomnie.
Portugal	Pas de statistiques. Données sur l'abonné, liste des numéros utilisés, données relatives au trafic.	Arnaques par hameçonnage, pédophilie sur Internet, autres infractions économiques liées à l'informatique.	Données sur l'abonné, liste des numéros utilisés, données relatives au trafic. Exemple : adresse IP, fuseau horaire, etc.	Accès illégal par des pirates, diffamation, vol de données.
Roumanie	Renseignements concernant des abonnés et informations connexes (journaux, localisation, équipement, etc.), données informatiques, données régie par la loi sur la conservation des données.	Essentiellement infractions liées à l'informatique (accès illégal, interférence avec des données, pédopornographie, etc.), ainsi qu'infractions liées à l'e-commerce. Statistiques : 95 demandes.	Renseignements concernant des abonnés et informations connexes (journaux, localisation, équipement, etc.), données informatiques, données régie par la loi sur la conservation des données.	Essentiellement infractions liées à l'informatique (accès illégal, interférence avec des données, pédopornographie, etc.), ainsi qu'infractions liées à l'e-commerce. Statistiques : 284 demandes.
Serbie	Renseignements concernant des abonnés essentiellement (journaux IP). *Fréquence* : 8 demandes en quatre ans.	Cyber-délits.	Renseignements concernant des abonnés (Bureau du Procureur spécial pour la cybercriminalité et Servies de Police) et données relatives au trafic (uniquement SPOC) *Fréquence* : 56 commissions rogatoires pour des demandes d'entraide entre 2008-2013 (SPOC), 3 demandes par la Police jusqu'ici.	Cyber-délits. Autres : menaces à la sécurité, fraude, contrefaçon et abus de cartes de paiement, instigation à la haine et à l'intolérance nationales, raciales et religieuses et terrorisme.

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
Slovaquie	Une seule demande d'entraide reçue en 2012/13 pour des renseignements spécifiques concernant des abonnés et des données relatives au trafic.	Fraude bancaire et informatique aggravée.	13 demandes en 2012 et 11 dans les cinq premiers mois de 2013 sur des données IP et autres données pour identifier des abonnés, des données relatives au trafic, transactions avec des cartes de paiement, mots de passe, contenu de messages électroniques.	Divers types de fraude, fausses cartes et fraude associée, blanchiment d'argent, diffamation etc.
Slovénie	Essentiellement renseignements concernant des abonnés, ainsi que des données relatives au trafic. *Fréquence* : environ 20 demandes en tout.	Typiquement infractions de fraude sur Internet, menaces sur Internet par courrier électronique, vol d'identité.	Essentiellement Renseignements concernant des abonnés, et une sur des données relatives au trafic. *Fréquence* : 4-5 demandes en tout.	Typiquement infractions de fraude sur Internet.
Espagne	Pas de statistiques. Essentiellement renseignements concernant des abonnés, ainsi que des données relatives au contenu, à l'hébergeur et liées à des moyens de paiement électroniques.	Essentiellement escroquerie, exploitation sexuelle d'enfants, menaces, infractions concernant l'intégrité des données et violations du droit de la propriété intellectuelle et industrielle.	Pas de statistiques. Essentiellement renseignements concernant des abonnés, ainsi que des données relatives au contenu, à l'hébergeur et liées à des moyens de paiement électroniques.	Essentiellement menaces et pédopornographie (en particulier informations concernant l'abonné ou sur le contenu).
Suisse	Pas de statistiques. Renseignements concernant des abonnés (adresses IP)	Fraude, fraude informatique, obtention non autorisée de données, accès non autorisé, [pédo]pornographie, trafic de	Pas de statistiques. Renseignements concernant des abonnés, données relatives au contenu.	Fraude, fraude informatique, obtention non autorisée de données, accès non autorisé, [pédo]pornographie, trafic de stupéfiants.

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
		stupéfiants.		
«ex-République yougoslave de Macédoine»	Renseignements concernant des abonnés, Données relatives au trafic. *Fréquence* : très petit nombre de cas seulement (2010-2013).	Pas de demande.	Données relatives au trafic et renseignements concernant des abonnés. *Fréquence* : 14 demandes d'entraide, essentiellement données relatives au trafic. 7 demandes pour des données relatives au trafic pour pédopornographie et 12 demandes liées à des vols d'identité	Accès illégal à un système informatique, infractions liées à l'accès illégal à un système informatique, pédopornographie, vol d'identité.
Turquie	Données sur des IP, localisation, enregistrement, paiement, autres informations et contenu. *Fréquence* : 7 demandes en 2011, 11 demandes en 2012.	Accès illégal, piratage de sites web, sabotage d'ordinateurs, fraude informatique, fabrication de faux sites web, insultes, menaces, diffamation, chantage.	Données sur des IP, localisation, enregistrement, paiement, autres information et contenu. *Fréquence* : 232 demandes en 2011, 364 en 2012.	Accès illégal, piratage de sites web, sabotage d'ordinateurs, fraude informatique, fabrication de faux sites web, insultes, menaces, diffamation, chantage, usage frauduleux de cartes de crédit, fraude aux paiements, violation de la vie privée, enregistrement et interception illégaux de communications, terrorisme, contrebande.
Ukraine	(MdI) Renseignements sur l'abonné, fichiers journaux, fichiers de systèmes de facturation, copies de serveurs etc. *Fréquence* : 4 demandes en 2014 jusqu'ici.	(MdI) Attaques par DDoS, accès non autorisé à des serveurs de services répressifs, vol de données d'administrations publiques etc. Par exemple, en 2011, demande de la France à la suite	(MdI) Renseignements sur l'abonné, fichiers journaux, fichiers de systèmes de facturation, copies de serveurs, propriétaires WMID, etc. *Fréquence* : pas de statistiques	(MdI) Tous types de délits liés à la cybercriminalité (Ser Sec) Participation à des équipes internationales de piratage, développement de logiciels malveillants, intrusion dans des systèmes

Pays	Demandes entrantes		Demandes sortantes	
	Informations demandées	**Types d'infraction**	**Informations demandées**	**Types d'infraction**
	(Ser Sec) Pas de statistiques, adresses IP, copies de disques durs, données relatives au trafic. *Fréquence* : 21 demandes en 2009, 18 en 2010, 11 en 2011, 28 en 2012, 11 en 2013 à ce jour.	d'une intrusion illicite dans des serveurs du Gouvernement. (Ser Sec) Pas de statistiques. Cyber-délits, délits financiers, avec spécificités régionales	(Ser Sec) Habituellement, renseignements sur des utilisateurs d'IP. Fréquence : 8 demandes depuis 2006 (6 en 2009, 1 en 2011, 1 en 2012).	bancaires, retraits d'espèces.
Royaume-Uni	Essentiellement renseignements concernant des abonnés, des factures de téléphones et des données sur les adresses IP. Autres : données relatives au contenu et interception en temps réel	Tout type d'infraction.	Essentiellement renseignements concernant des abonnés, des factures de téléphones et des données sur les adresses IP. Pas de statistiques.	[à clarifier]
États-Unis	Données relatives au trafic, données sur l'abonné, contenu du service hébergeur, courriers électroniques stockés. *Fréquence* : des centaines de demandes par an.	Essentiellement cyber-délits classiques (fraudes à la carte de crédit, intrusion informatique), et crimes violents (kidnapping, fusillades, terrorisme, menaces à la bombe).	Données relatives au trafic, données sur l'abonné et courriers électroniques stockés. *Fréquence* : des centaines de demandes par an.	Tout type de crime ; essentiellement cyber-délits classiques.

2.5.2 Demande d'entraide contre coopération entre polices (Question 1.3) et information spontanée (Question 1.4)

1.3 Entraide contre coopération entre polices

Sur la base de la législation de votre pays et de votre expérience pratique, quelle différence faites-vous entre l'entraide et l'échange d'informations entre polices concernant des données informatiques stockées ?

Quel type d'informations (y compris des données informatiques stockées) pourriez-vous transmettre dans le cadre de la coopération entre polices en l'absence ou en amont d'une demande d'entraide ? À quelles conditions serait soumise la transmission de ces informations ?

1.4 Information spontanée (article 26)

L'article 26 porte sur l'envoi d'informations à un autre État en l'absence de demande d'entraide. Selon quelle fréquence envoyez-vous ou recevez-vous des informations spontanées ?

D'après votre expérience, quelle est l'utilité de ces informations et quelles suites leur donnez-vous ? Veuillez donner des exemples pour illustrer la façon dont cette possibilité est utilisée.

Pays	**Entraide judiciaire contre coopération entre polices (Q 1.3)**		**Information spontanée (Q 1.4)**
	Différence	**Données fournies sans demandes d'entraide**	
Albanie	Coopération policière : - plus rapide ; - évite les conditions formelles de l'entraide et la nécessité d'accords bilatéraux.	Uniquement les données opérationnelles générées par le travail de police.	- Fréquence : pas très souvent. - Utilisation/pertinence : aider à démarrer une procédure pénale ou à présenter une demande d'entraide émanant d'autorités étrangères - Suivi : toutes informations supplémentaires sont fournies aux autorités étrangères.
Arménie	La demande d'entraide n'est possible que si une affaire pénale a été intentée. On se sert des 24/7 et de la coopération entre polices pour obtenir les informations suffisantes au	Les données relatives au trafic peuvent être fournies sans demande d'entraide, sur demande officielle décrivant l'affaire et les informations souhaitées. Si celle-ci arrive sans	

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
	déclenchement des poursuites pénales. La plupart des demandes restent sans réponse. D'autres pays exigent une demande d'entraide.	décision de justice, il est possible d'obtenir une injonction en Arménie.	
Australie	Pour les demandes sortantes, une demande d'entraide est nécessaire afin que les données respectent les conditions d'admissibilité de l'Australie dans des poursuites devant des tribunaux australiens. Les données obtenues par le biais de la police ne peuvent servir qu'aux fins de l'enquête. Pour les demandes entrantes, une demande d'entraide est nécessaire lorsque l'assistance implique le recours à la coercition (exemple des demandes pour des données de télécommunications prospectives).	Journaux IP et données sur l'abonné obtenus auprès des FSI. Dans certaines circonstances, la police peut exiger la conservation des données relatives au contenu au nom d'un service répressif étranger, en attendant une demande d'entraide.	- Fréquence : pas de données statistiques. - Utilisation/pertinence: en général, plutôt intra-services qu'entre gouvernements. L'autorité centrale peut faciliter la liaison entre les services répressifs.
Autriche	Une demande d'entraide judiciaire est nécessaire pour obtenir de données relatives au trafic ou au contenu.	- Données qui, de par leur nature, doivent être transmises en vertu du droit international ; - Données demandées par des services répressifs étrangers pour s'acquitter de leurs missions, sous condition de réciprocité ;	- Fréquence : pas de données statistiques - Utilisation/pertinence : des informations qui pourraient aboutir à une enquête criminelle pour une infraction relevant de la juridiction nationale sont transmises au procureur compétent. - Suivi : le résultat de l'enquête (la condamnation) est communiqué à l'autorité étrangère qui a fourni les informations.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
		- Données demandées par Interpol pour une enquête criminelle.	
Belgique	La différence réside dans l'objectif final. La coopération judiciaire a pour but d'obtenir des preuves en vue de les utiliser dans des procédures pénales. En principe, les informations reçues ou transmises par le biais de la coopération policière n'engagent pas les autorités judiciaires et ne peuvent être utilisées comme preuves.	La coopération policière est en principe limitée au gel de données stockées. Pour la transmission, il faut une commission rogatoire à moins que la police n'ait déjà obtenu les données dans le cadre d'une enquête en Belgique. Si les mêmes données sont nécessaires à une autre juridiction, le magistrat compétent pourrait autoriser leur transmission à des autorités étrangères.	Si des informations spontanées sont reçues par le Service contre la criminalité High Tech, un procès-verbal est établi et transmis au parquet.
Bosnie-Herzégovine	Différents cadres juridiques s'appliquent. Ainsi, les FSI ne sont pas obligés de fournir des données sur demande directe de la police, sans mandat judiciaire.	Données opérationnelles détenues par la police, à condition qu'aucune injonction judiciaire ne soit exigée (dépend des problèmes liés au respect de la vie privée).	- Fréquence : pas de données statistiques (aucun cas au titre des PC 24/7, certains cas via les canaux d'INTERPOL). - Utilisation/pertinence : chaque fois que des données opérationnelles ou des preuves concernant une infraction pénale, commise ou en préparation dans un autre État, sont disponibles (essentiellement adresses IP). - Suivi : de toute action prise par la suite. Obligatoire en droit national.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Bulgarie	Les données obtenues par le biais d'une coopération policière ne peuvent être utilisées au tribunal. Des mécanismes spécifiques s'appliquent pour les demandes d'entraide au sein de l'UE.	- Informations et données provenant des sources d'information du ministère de l'Intérieur ; - Informations ou données reçues d'autres organismes étatiques ou pouvoirs locaux, de personnes morales et de personnes physiques. *Conditions* : - applicable aux relations avec les États membres et signataires de l'Accord de Schengen ; - application des critères nationaux (voir art. 161 e de la nouvelle Loi sur le MoI – SG 93/09).	- Fréquence : n/a. [à clarifier] - Utilisation/pertinence : dépend de l'information. Le partage de modus operandi, bonnes pratiques ou exemples est utile. Les informations peuvent aboutir au déclenchement de poursuites pénales (trafic illicite de biens culturels, blanchiment d'argent, fausse monnaie, délit lié à un ordinateur, traite des êtres humains, exploitation sexuelle des enfants etc.)
Costa Rica	Le Bureau du Procureur général traite les demandes d'entraide. Ceci n'exclut pas la coordination avec les organisations de police (par exemple Interpol).	Pas de données sans mandat judiciaire.	- Fréquence : pas de données statistiques - Utilisation/pertinence : très important, par exemple pour définir des stratégies d'enquête pour de futures demandes d'assistance pénale internationale.
Croatie	L'échange spontané d'informations est régi par l'article 18 de la Loi et doit être réalisé selon les règles applicables en matière de droits de l'homme et de protection des	Informations générales sur les délinquants et les infractions (base de données du MdI). Données émanant d'institutions étatiques (lorsque cela est autorisé sans injonction	- Fréquence : pas de données. - Utilisation/pertinence : chaque fois que les données peuvent aider à déclencher ou à poursuivre une enquête ou des procédures judiciaires, ou aboutir à la présentation d'une demande d'entraide. - Suivi : de toute action ultérieure. Obligatoire en droit national.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
	données personnelles. Ces informations pourraient être utilisées pour entamer des enquêtes ou intenter des poursuites pénales. L'utilisation de ces données en justice en tant que preuve n'est pas autorisée sans demande d'entraide (commission rogatoire), ce qui vaut pour les demandes entrantes et sortantes. Les données stockées ne peuvent être conservées par la police qu'à titre temporaire pendant 90 jours (puis 90 jours supplémentaires en cas de prorogation), mais pour qu'elles puissent être transmises à l'État requérant, il faut une demande formelle.	judiciaire) ; données obtenues par le biais d'auditions.	
Chypre	Toutes données pour lesquelles un mandat n'est pas nécessaire à Chypre peuvent être fournies sans demande d'entraide, y compris les adresses IP [cela veut-il dire des infos sur l'abonné ?] et des données du registre des sociétés.	Les données sur l'enregistrement d'une société, le casier judiciaire et des informations personnelles sur les propriétaires de véhicules et de navires peuvent être communiquées sans demande formelle d'entraide.	Le Service de lutte contre la Cybercriminalité expédie environ 50 lettres par an avec ce type d'informations et en reçoit environ 35. Les informations sont fournies à des fins d'analyse et de mesures proactives.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
République dominicaine	Demande d'entraide si les données doivent être utilisées dans des procédures judiciaires.	Données sur adresses IP ou abonnés téléphoniques ou sur des sites web locaux s'ils sont hébergés en République dominicaine et avec l'aide du ministère public.	Des informations sont échangées en particulier avec les pays participant au Forum ibéro-américain des forces de cyberpolice (Foro Iberoamericano de Encuentro de Ciberpolicías, Fiec). Cela a permis de monter une coopération réussie entre plusieurs pays, et d'arrêter plus de 25 membres d'Anonymous.
Estonie	- La coopération policière s'applique à l'échange de données qui sont disponibles publiquement ou dans les bases de données de l'État ; - Si les données ne peuvent être obtenues par ce moment ou qu'il faut des actes de procédure particuliers, une demande d'entraide est nécessaire.	Informations disponibles publiquement ou dans les bases de données de l'État.	- Fréquence : Pas de statistiques. Ce processus est autorisé, mais rarement utilisé. - Utilisation/pertinence : dépend du contenu et de la qualité des informations dans une affaire spécifique. Par exemple des informations sur des biens piratés vendus sur un site web, si on n'a pas de détails sur les biens, les victimes et la relation avec l'État demandeur, ont un intérêt limité.
Finlande	- La coopération policière est essentiellement utilisée pour diriger des enquêtes en cours (trouver le meilleur moyen de recueillir des preuves). - La demande d'entraide concerne l'échange officiel d'informations et exige de recueillir des preuves. Seuil pour activer l'entraide : lorsque l'enquête criminelle démarre (lorsqu'on a des raisons de soupçonner qu'un délit pénal a été commis).	Différents types d'informations, aux fins visées par Q 1.3.1. Les données ne peuvent être fournies lorsqu'elles ne peuvent être obtenues que par des mesures coercitives.	Informations non disponibles.
France	- La demande d'entraide peut	Toutes données qui peuvent être	- Fréquence : très rare.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
	concerner la coopération officielle (par Interpol, Europol ou les canaux du G8), les éléments étant destinés à être utilisés dans des enquêtes et poursuites judiciaires ; - La coopération policière (via les officiers de liaison ou autres) est plus informelle. Elle peut donner des indications pour les enquêtes. Les éléments recueillis ne peuvent pas servir de preuves dans des procédures judiciaires.	obtenues sans qu'il soit nécessaire de délivrer une injonction ou d'entreprendre des mesures coercitives.	- Exemple : informations fournies par l'Allemagne concernant des serveurs compromis, notamment une liste des adresses IP des clients. Le fournisseur de services d'hébergement a été contacté et la liste de clients lui a été communiquée pour qu'il les informe.
Géorgie	- La demande d'entraide est régie par la loi sur la coopération entre les autorités judiciaires ; - la coopération policière est régie par la loi sur la coopération entre services répressifs.	Données contribuant à la prévention, à la détection et à l'élimination des délits ; données sur des personnes recherchées, participant ou soupçonnées de participer à une infraction ; connexions, organisation et modus operandi des délinquants, etc. ; acquisition et enregistrement d'armes à feu ; identification de véhicules à moteur et de son propriétaire/ses utilisateurs ; renseignement criminel etc.	Fréquence : pas de statistiques. Utilisation dans certaines occasions. Utilisation/pertinence: - (Envois) utiles lorsque les services répressifs estiment que les informations présentent un intérêt pour l'État étranger, à condition que la transmission des informations soit compatible avec le droit interne ; - (Réceptions) très utiles pour l'enquête sur des délits complexes (ex. crime organisé transnational), soit pour donner une certaine direction à l'enquête, soit pour fournir des preuves supplémentaires afin de traduire un suspect en justice.
Allemagne	Les données nécessaires pour des poursuites pénales doivent être demandées par le biais d'une	Données sur l'abonné, sous condition de réciprocité.	Fréquence : Informations envoyées quotidiennement ; réceptions aussi (pas de statistiques disponibles).

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
	demande d'entraide judiciaire.		
Hongrie		Des données sur l'abonné peuvent être transmises sans demande d'entraide.	Pas d'expérience. Jamais envoyé ou reçu de demande de ce type
Islande	Les données nécessaires pour des poursuites pénales doivent être demandées par le biais d'une demande d'entraide judiciaire.	Un large éventail d'information lorsqu'une enquête est en cours mais également des informations de renseignement ?	Ce type d'information est habituellement transmis au niveau de la police et non par le Ministère. Donc aucune information n'est disponible.
Italie	Distinction basée sur le caractère informel de la demande	n/a.	Utilisation/pertinence : uniquement pour des données relatives à des cyberattaques ou cyber-menaces. Ne s'applique pas pour des données stockées. Exemple : après vérification, des informations sur la planification d'une cyberattaque par un groupe de hackers sont transmises au système ou réseau ciblé.
Japon	- Utilisation de l'entraide lorsque la demande concerne la fourniture de preuves ou demande des mesures obligatoires ; - Coopération policière pour les autres cases.	Pour les données ne concernant pas la fourniture de preuves, et pour lesquelles il n'est pas exigé une enquête obligatoire.	Pas pratiqué.
Lettonie	La coopération policière est nécessairement suivie par une demande d'entraide, si les données stockées doivent servir de preuve.	Pas de données, hormis si elles ont été déjà obtenues dans le cadre d'enquêtes nationales et ont fait l'objet d'une transmission spontanée d'informations.	- Fréquence : très souvent. - Exemple : Information sur des « mules » pour le transport d'argent. - Suivi : habituellement, déclenchement d'une enquête.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Lituanie	Les informations obtenues par le canal de la coopération policière (internationale) sont utilisées pour le renseignement policier. Exception : lorsque le fournisseur étranger des informations autorise l'utilisation des données comme preuve.	Tout type d'information, y compris des données informatiques stockées, qu'il n'est pas interdit de collecter et de fournir sans autorisation officielle du Procureur ou de la Justice et en vertu d'autres dispositions du droit interne.	non pratiqué.
Malte			Les envois/réceptions d'informations spontanées sont rares et, dans ce cas, se font par des canaux tels qu'Europol ou Interpol, et une fois par le biais d'un point de contact 24/7. Les informations concernent en général des éléments de pédopornographie téléchargés ou des utilisateurs dont les ordinateurs sont infectés par des logiciels ou programmes malveillants. Souvent, les informations sont envoyées après la durée légale de conservation des données (6 mois) et les données nécessaires ne sont plus disponibles, ce qui empêche d'identifier les utilisations.
Moldova	- Toutes les demandes en poursuites pénales sont adressées au Procureur général ; - Toutes les demandes effectuées durant un procès ou l'exécution d'une sentence sont adressées au ministère de la Justice.	Uniquement des données opérationnelles créées durant le travail de police.	n/a.
Monténégro	Pas de données.	N'importe quelles données, en fonction de l'infraction pénale et des conditions exigées par le droit procédural interne.	- Fréquence : pas de données. - Utilisation/pertinence: n/a.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Pays-Bas	Le parquet est chargé de faire la demande d'entraide pour obtenir des données informatiques stockées. - Les demandes de conservation sont reçues par le biais du point de contact 24/7 ; - Les demandes de transfert de données conservées sont reçues par le biais de l'AIRS (autorité centrale) ou de l'IRC (bureau chargé de l'entraide internationale en matière pénale).	- Les données conservées sur instruction du procureur peuvent être partagées par le biais de la coopération policière en attendant une demande formelle, mais uniquement à des fins d'enquête et avec l'accord du procureur (affaires très urgentes seulement) ; - Les données conservées sur injonction du juge d'instruction ne peuvent être transférées formellement qu'avec l'accord du tribunal compétent.	Envois d'informations : Fréquence : approx. 3 fois par mois. Utilisation/pertinence : on va aussi vite et aussi loin que possible étant donné que l'État qui bénéficiera des informations en attend beaucoup. Réception d'informations : Fréquence : pratiquement jamais, vraisemblablement du fait d'obstacles juridiques. Utilisation/pertinence : pas assez pratiqué.
Norvège	- L'échange of données relatives au contenu exige en général une demande d'entraide ; - il est possible d'échanger certaines données par le biais de la coopération policière (par exemple, renseignements concernant des abonnés) sans demande formelle ou injonction du tribunal, mais c'est plus facile en cas d'enquêtes mutuelles ou parallèles.	- large gamme d'informations, lorsqu'une enquête liée est en cours au niveau national ; - certaines informations (par exemple, renseignement).	Fréquence : Pas de statistiques. Utilisation/pertinence: - peut avoir de l'importance dans de nombreux cas, en tant que renseignement (modus operandi) ou pour démarrer une enquête criminelle ; Exemple : informations sur un logiciel ou programme malveillant découvert durant une enquête criminelle sur des intrusions informatiques. - peut être transférées par Europol ou des mécanismes similaires. Suivi : dépend des informations (pertinence pour une affaire/projet en cours)

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Philippines	La demande d'entraide est utilisée chaque fois que des documents probants émanant d'une juridiction étrangère sont nécessaires pour poursuivre efficacement des affaires intentées dans le pays ou qui font l'objet d'une enquête ; le recueil de renseignement est effectué chaque fois que des informations provenant d'autres juridictions sont utiles pour identifier et déterminer l'implication d'un suspect dans un acte illégal ou essentiellement pour construire l'affaire. La coopération policière se fait suite à une demande officielle, mais sans nécessité d'intervention judiciaire. Les données partagées sont toutefois limitées et ne peuvent servir de preuve dans le cadre d'une quelconque procédure sans avoir reçu le consentement prépalable de l'Etat requis/	Uniquement des preuves d'activités illégales de ressortissants étrangers et des rapports de renseignement. Pour les données informatiques stockées, il faut une injonction de justice, et elles ne peuvent donc pas être utilisées par d'autres juridictions si elles ne respectent pas les conditions de l'entraide.	Des informations spontanées sont souvent reçues de la part des attachés de police de juridictions étrangères affectés localement. Le recueil et le partage d'information ne recouvre pas uniquement les demandes d'informations, il y a toujours une étroite coopération et coordination entre le Service judiciaire des Philippines et la police et les attachés de police de différents pays.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Portugal	L'obtention de données est soumise à l'autorisation de l'autorité judiciaire.	Aucune.	Utilisation/pertinence : toutes informations de police sont transmises, à condition qu'il ne soit pas obligatoire de faire une demande judiciaire. Les informations reçues ont très importantes et aboutissent souvent à l'ouverture d'une affaire criminelle.
Roumanie	- Différents cadres juridiques s'appliquent, et les dispositions légales sur la coopération judiciaire priment sur les dispositions relatives à la coopération policière ; - La coopération policière se concentre sur les demandes pour l'échange de données opérationnelles, les informations sur des infractions, etc. ; - La coopération policière est souvent nécessaire au début d'une enquête.	- données personnelles émanant de bases de données nationales (par exemple, casiers judiciaires), informations, renseignements détenus dans la base de données policières.	- Fréquence : pas très souvent. - Utilisation/pertinence : les demandes sont envoyées/reçues en vertu des accords internationaux applicables. Les demandes reçues sur la base de la Convention de 1959 relative à l'entraide sont analysées et transmise par les autorités centrales aux autorités judiciaires compétentes (bureau local du procureur). Il faut plus d'expérience pour évaluer cet outil. - Exemple : des informations reçues sur une affaire de fraude informatique commise par un ressortissant, transmises au Bureau du Procureur attaché à la Cour suprême de cassation et de justice.
Serbie	La coopération policière : - est beaucoup plus rapide ; - évite les conditions formelles de l'entraide et la nécessité d'accords bilatéraux.	Données opérationnelles détenues par la police, à condition qu'il ne soit pas obligatoire d'avoir une injonction d'un tribunal.	- Fréquence : très souvent. - Utilisation/pertinence : chaque fois que des informations sur des activités criminelles peuvent présenter un intérêt pour des autorités étrangères, et réciproquement. - Suivi : toutes informations supplémentaires sont transmises aux autorités étrangères.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Slovaquie	Pour l'entraide, il faut des poursuites pénales. Au contraire, la coopération policière sert à obtenir des informations nécessaires pour que la police puisse exercer sa mission et les informations qui pourraient permettre d'entamer des poursuites pénales. Les résultats obtenus par la coopération policière ne peuvent en revanche pas être utilisés comme preuve dans des poursuites pénales.	Seules des informations concernant des renseignements criminels peuvent être échangées avec la police. L'accès aux données de trafic/relatives au contenu, adresses IP, journaux etc. dans des procédures pénales est réglementé. Ces données sont régies par le secret des télécommunications, encadré par une loi distincte, et l'accès à ces données doit être d'abord autorisé par la justice.	Jusqu'ici, l'article 26 de la Convention de Budapest n'est pas utilisé pour l'échange spontané d'informations, mais un jour ou l'autre, il finira par l'être, comme des dispositions similaires dans d'autres traités.
Slovénie	Les données obtenues par le biais de la coopération policière doivent d'abord être validées avant d'être utilisées en justice comme preuves.	Informations extraites des bases de données de l'État ; informations déjà obtenues dans certaines affaires nationales.	- Fréquence : très rare. - Utilisation/pertinence : peut permettre d'ouvrir une nouvelle affaire, lorsque les informations caractérisent une infraction en droit interne. Des preuves supplémentaires peuvent être utilisées dans des poursuites pénales.
Espagne	- La demande d'entraide est introduite par les autorités judiciaires dans le cadre de poursuites judiciaires ; - la coopération policière concerne les enquêtes policières (autrement dit avant les poursuites).	Uniquement les données techniques liées aux connexions.	- Fréquence : pas d'expérience. - Utilisation/pertinence : informations seraient immédiatement transférées au bureau compétent du Procureur. Au niveau policier, cela peut déclencher une enquête (en particulier dans des affaires de fraude, de cyberattaques et de pédopornographie).

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Suisse	- La demande d'entraide concerne le traitement des demandes émanant des autorités judiciaires et entraînant des mesures contraignantes et obligatoires [à clarifier] - La coopération policière concerne le traitement des demandes émanant des autorités de police du fait de leur propre compétence et non contraignantes ou obligatoires au niveau procédural (renseignements concernant des abonnés, etc.)	- Données concernant les titulaires d'adresses IP et données techniques accessoires qui sont disponibles sans mesures contraignantes et obligatoires ; - (en général) aucune restriction au type de données pouvant être transmises, à condition que cela concerne la lutte contre la criminalité et que les droits fondamentaux et principes des droits nationaux soient respectés.	- Fréquence : pas de statistiques. 5-10 envois par semaine sur pédopornographie, environ une réception par mois. - Utilisation/pertinence: Les informations envoyées concernent essentiellement la pédopornographie. (par exemple, des publicités pour des sites web contenant ce type de contenu) Les informations reçues concernent essentiellement soit le modus operandi d'un groupe criminel (par exemple des informations envoyées par Interpol Moscou sur une arnaque appelée *Epouse russe*), soit des informations sur une affaire criminelle spécifique, permettant aux services répressifs d'anticiper un délit (par exemple informations du FBI sur des préparatifs pour une attaque par déni de service) ou d'entamer une enquête (par exemple des sites web pédopornographiques hébergés dans le pays)
«ex-République yougoslave de Macédoine»	Coopération policière et entraide sont étroitement connectées, en particulier dans des affaires urgentes.	Uniquement pour établir la disponibilité des données et leur type.	- Fréquence : aucun cas. - Utilisation/pertinence : très utile pour résoudre des affaires dans lesquelles les données stockées sur informatique sont essentielles ; cela gagne du temps lorsque les données sont particulièrement fragiles.
Turquie	[à clarifier]	Uniquement des renseignements concernant des abonnés. (Pour les données relatives au trafic et données relatives au contenu, il faut l'accord des autorités judiciaires.)	- Fréquence : Pas de données. Cette pratique n'est pas rare. - Utilisation/pertinence : assistance d'autorités judiciaires étrangères ; transmission de renseignement criminel dans des affaires urgentes (avec menace pour la vie de quelqu'un), uniquement pour une utilisation policière.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
Ukraine	(MdI) - L'échange de données ne peut se faire que par l'entraide ; - La conservation des données peut être demandée par la Division Cybercriminalité du MdI. (Serv Sec) Les informations obtenues par l'entraide peuvent être utilisées comme preuves en justice.	(MdI) Aucunes données ne peuvent être obtenues de FSI ou autres personnes morales/physiques sans une injonction judiciaire. (Serv Sec) Uniquement les informations qui ne contiennent pas de données personnelles ou données liées à des données personnelles.	(MdI) - Les informations peuvent être envoyées si, ce faisant, on ne viole pas les droits des personnes privées, le secret des détenteurs de données privés et la loi sur le secret d'Etat. - Utilisation/pertinence : peuvent être très pertinentes (données analytiques reçues à partir d'une source ouverte, données statistiques traitées par des services de lutte contre la cybercriminalité, etc.) (Serv Sec) - Fréquence : envois réguliers d'informations, essentiellement concernant des affaires de fraude. Demandes régulières d'informations également (40 à 70 demandes par an). - Utilisation/pertinence : les informations sont pertinentes dès lors qu'elles concernent les activités illégales de ressortissants ou sont demandées par un partenaire.
Royaume-Uni	- Il existe des règles formelles à appliquer pour une demande d'entraide ; - Le partage d'informations dans le cadre d'une coopération policière sert au renseignement.	Données auquel on a accès via la coopération entre services de police. [à clarifier]	- Fréquence : pas de statistiques. - Suivi : aucun suivi, à moins de demande particulière en ce sens. La validité et la proportionnalité de la demande sont contrôlées.

Pays	Entraide judiciaire contre coopération entre polices (Q 1.3)		Information spontanée (Q 1.4)
	Différence	**Données fournies sans demandes d'entraide**	
États-Unis d'Amérique	Une demande d'entraide est nécessaire chaque fois qu'il faut une injonction judiciaire pour obtenir les données. (*Voir colonne de droite pour plus de détails*)	- La conservation peut être obtenue par l'intermédiaire de la police ou directement par l'autorité étrangère ; - les informations ne concernant pas le contenu peuvent être obtenues directement avec l'accord du fournisseur ; - des informations obtenues dans le cadre d'une enquête ou de poursuites nationales, sous réserve de limites et prescriptions ; - des informations sur le contenu, avec l'aide des services répressifs locaux, en cas d'urgence et avec l'accord du fournisseur.	Fréquence : en permanence, même si on ne les appelle pas comme çà. Utilisation/pertinence: utiles - Cette « étiquette » permet de fournir des informations potentiellement utiles sans que l'Etat étranger ne soit obligé d'introduire une demande d'entraide ; - elle peut réduire la nécessité d'introduire une demande d'entraide, étant donné qu'une partie des informations nécessaires a déjà été transmise à l'Etat étranger.

3 Évaluation des procédures et des conditions régissant l'entraide pour ce qui est de l'accès à des données stockées.

3.1 Conditions

Les réponses au questionnaire énumèrent une série de conditions.

Forme de la demande :

- La demande se fait par écrit ou sous forme électronique à condition que son authenticité puisse être établie.
- Conditions de langue prévues dans l'instrument juridique (voir plus loin).
- Transmission par les moyens et les autorités prévus dans l'instrument légal sur lequel se base la demande.

Contenu de la demande[12] :

- Nom de l'autorité requérante et si possible détails concernant les autorités requises responsables de l'exécution de la demande.
- Fondement juridique étayant la demande (en général les dispositions légales internes au pays régissant la coopération internationale en matière pénale et la procédure pénale liée à des accords bilatéraux sur l'entraide, la Convention de Budapest sur la cybercriminalité, la Convention européenne d'entraide pénale et autres traités du Conseil de l'Europe ; les traités internationaux des Nations-Unies et autres, ou la réciprocité).
- Buts et motifs de la demande.
- Nécessité de la demande.
- Identification de l'infraction et droit applicable.
- Résumé des faits et des chefs d'accusation.
- Information sur les personnes concernées.
- Mesures demandées.
- Description des preuves recherchées et informations à cet égard (les données stockées recherchées et leur relation avec l'infraction, les numéros de téléphone ou adresses IP impliqués ; le moyen utilisé pour la communication électronique, la période de temps couverte par la demande de données, etc.).
- Identification de la personne physique ou morale détenant les données recherchées.
- Adjonction en annexe de la décision judiciaire, par exemple injonction de divulgation de données relatives au contenu.
- Informations pertinentes pour l'examen d'une éventuelle intrusion dans la vie privée de tiers et modalités destinées à l'atténuer (Royaume-Uni).

Conditions prévues par le droit interne du pays :

- Conformité de la demande et des mesures à prendre avec le droit interne, en particulier pour ce qui est des mesures contraignantes.
- Principe de la double incrimination (Finlande[13], Géorgie, Allemagne, Hongrie, Japon, Norvège, Serbie, Suisse, États-Unis peu fréquemment).

---

[12] Voir aussi l'énumération à l'article 29 de la Convention de Budapest.

- La demande doit être liée à un crime ou à une infraction graves (Espagne).
- Principe de la « cause probable » pour une demande concernant des données relatives au contenu (États-Unis).
- Injonction d'un tribunal ou décision d'un procureur, en fonction du type d'informations demandées.

Le tableau suivant indique l'institution pouvant autoriser l'accès à des données stockées au niveau national à la suite d'une demande d'entraide émanant d'une juridiction étrangère.

Autorisation d'accès à des données informatiques stockées, en cas de demande d'entraide[14] émanant d'une juridiction étrangère

Pays	**Données relatives à l'abonné**	**Données relatives au trafic**	**Données relatives au contenu**
Arménie	Procureur	Procureur	Procureur
Australie	Police	Police	Officier judiciaire (après autorisation de l'Attorney-General)
Azerbaïdjan	Tribunal	Tribunal	Tribunal
Belgique	Procureur	Tribunal	Tribunal
Bosnie-Herzégovine	Tribunal	Tribunal	Tribunal
Estonie	Police	Procureur	Tribunal
Finlande	Police/Tribunal	Tribunal	Tribunal/ Police[15]
Allemagne	Police (aussi Procureur/Tribunal)	Tribunal (dans des circonstances exceptionnelles : le Procureur également)	Tribunal (dans des circonstances exceptionnelles : le Procureur également)
Hongrie	Police	Police	Tribunal
Japon	Police/Tribunal	Tribunal	Tribunal
Lettonie	Procureur/Tribunal	Procureur/Tribunal	Procureur/Tribunal
Lituanie	Police (également Procureur/Tribunal)	Tribunal (Décision du Procureur approuvée par le Juge d'instruction intervenant préalablement au procès)	Tribunal
Moldova	Procureur	Tribunal	Tribunal
Philippines	Tribunal	Tribunal	Tribunal
Portugal	Procureur (police en cas d'urgence)	Tribunal	Tribunal

[13] Observation de la Finlande : de manière générale, le principe de la double incrimination s'applique en Finlande, si des mesures coercitives sont demandées.

[14] Tableau simplifié. Pour les détails, voir réponses au questionnaire.

[15] Les autorités de police peuvent saisir un document. Ceci est différent de l'obtention du contenu de messages, où la décision incombe à la justice.

Roumanie	Tribunal	Tribunal	Tribunal
Serbie	Procureur	Tribunal	Tribunal
Slovaquie	Tribunal, plus précisément le Président de la Chambre du tribunal (avant le déclenchement des enquêtes criminelles) ou le Procureur (dans le cadre des procédures préparatoires), le Code pénal slovaque (n° 301/2005 Coll. tel qu'amendé) ne faisant pas la différence entre renseignements concernant les abonnés et données relatives au trafic.	Tribunal, plus précisément le Président de la Chambre du tribunal (avant le déclenchement des enquêtes criminelles) ou Procureur (dans le cadre des procédures préparatoires)	Tribunal
Slovénie	Police/Tribunal	Tribunal	Tribunal
États-Unis d'Amérique	Tribunal (sauf si le FSI fournit volontairement les données)	Tribunal (sauf si le FSI fournit volontairement les données)	Tribunal

3.2 Motifs de refus

La Convention de Budapest, dans ses articles 25 et 27, traite des motifs de refus de la coopération:

Article 25 – Principes généraux relatifs à l'entraide

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante[16].

[16] Extrait du Rapport explicatif :

"259. Pour l'essentiel, le paragraphe 5 donne une définition de la double incrimination aux fins de l'entraide au sens de ce chapitre. Lorsque la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination (par exemple lorsqu'elle s'est réservé le droit d'exiger la double incrimination comme condition pour exécuter une requête de conservation des données en application du paragraphe 4 de l'article 29, "Conservation rapide de données informatiques

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

Dans leurs réponses, les États indiquent les motifs de refus suivants :

- les motifs énumérés à l'article 27 de la Convention de Budapest.
- La demande ne respecte pas des critères formels ou autres (voir section précédente).
- La demande est motivée par la race, la religion, l'orientation sexuelle, l'opinion politique ou motif de même ordre.
- La demande concerne une infraction/délit politique ou militaire.
- La coopération peut entraîner des actes de torture ou la peine de mort.
- L'exécution de la demande serait préjudiciable à la souveraineté, à la sécurité, à l'ordre public ou aux intérêts nationaux ou autres intérêts essentiels.
- La personne a déjà été sanctionnée ou acquittée ou graciée pour le même délit (« Ne bis in idem »).
- L'enquête entraînerait une charge excessive pour l'Etat requis ou créerait des difficultés pratiques.
- Le fait d'exécuter la demande interférerait avec une enquête en cours (auquel cas, l'exécution de la demande peut être repoussée).
- Risque de poursuites discriminatoires (Pays-Bas).
- La demande concerne la liberté d'expression (États-Unis).
- Les procédures ne respectent pas la Convention européenne des droits de l'homme (Portugal).
- Les informations demandées sont liées à la sécurité nationale (Slovénie).

---

stockées"), cette condition sera considérée comme satisfaite si le comportement constituant l'infraction en relation avec laquelle l'entraide est requise est également qualifié d'infraction pénale par le droit interne de la Partie requise, même si ledit droit interne classe l'infraction dans une catégorie d'infractions différente ou la désigne en utilisant une terminologie différente. Cette disposition a été jugée nécessaire afin de garantir que les parties requises ne recourent pas à un critère trop rigide lorsqu'elles appliquent la double incrimination. Étant donné les différences entre les ordres juridiques nationaux, on ne s'étonnera pas de constater des différences de terminologie et de classement des comportements criminels. Si le comportement constitue une infraction pénale dans les deux ordres juridiques, ces différences d'ordre technique ne devraient pas empêcher l'octroi de l'entraide. Dans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance. »

Conclusions préliminaires :

- Certains États peuvent refuser la coopération si l'affaire est de moindre importance ou que cela fait peser une charge excessive sur les services d'enquête. Or, cela pose problème puisque les seuils ne sont pas formalisés et ne sont pas transparents pour les autres Parties. Il est certes possible que les ressources requises pour une coopération portant sur une petite affaire soient parfois disproportionnées, mais des petites affaires peuvent faire partie d'affaires plus conséquentes ou liées à des organisations criminelles. Si on applique des seuils, alors il faut davantage de transparence et de dialogue avec la Partie requérante.

- Comme indiqué plus haut, un certain nombre de Parties exigent la double incrimination pour ce qui est des demandes d'entraide concernant des données informatiques stockées. En vertu de l'article 25.5 de la Convention de Budapest et du Paragraphe 259 du Rapport explicatif, les Parties sont encouragées à adopter une approche flexible lors de l'application du critère de double incrimination, en particulier concernant les infractions visées aux articles 2 à 11 de la Convention de Budapest.

- Certaines Parties refusent de coopérer lorsque la demande concerne certains contenus, par exemple le discours de haine ou la pornographie.

3.3 Langue dans laquelle est formulée la demande

La question de la langue de rédaction des demandes d'entraide internationale est pour la plupart des États un problème majeur, essentiellement du fait :

- des retards induits par les traductions ;
- du coût des traductions ;
- de la qualité limitée des traductions, notamment une terminologie peu claire ;
- de la maîtrise limitée de langues étrangères par les praticiens.

Même si, à des fins internes (motifs juridiques et pratiques), des traductions certifiées resteraient nécessaires, la plupart des États acceptent une demande rédigée en anglais, à l'exception du Costa Rica (espagnol), de la République dominicaine (espagnol), de l'Allemagne (allemand), du Japon (japonais), de la Slovaquie (slovaque), de l'Espagne (espagnol), à moins que d'autres langues ne soient prévues au titre d'accords différents.

Conclusions préliminaires :

- un Protocole additionnel à la Convention de Budapest pourrait prévoir que les demandes d'entraide judiciaire envoyées en anglais sont acceptées par les Partis, du moins en cas d'urgence.

- les demandes d'entraide concernant la cybercriminalité et la preuve électronique pourraient être harmonisées :

  - l'utilisation de formulaires standard réduirait les besoins de traductions (des en-têtes ou champs standard n'auraient pas à être traduits) ;

  - le recours à un glossaire multilingue pour les termes techniques améliorerait la qualité des demandes.

Etat	**Langue requise ou acceptée[17] pour la réception d'une demande d'entraide**
Albanie	albanais, anglais
Arménie	anglais, russe, arménien
Australie	anglais
Autriche	allemand, anglais ou français
Azerbaïdjan	Anglais, russe, turque
Belgique	anglais
Bosnie-Herzégovine	bosniaque, croate ou serbe, anglais toléré pour le canal Interpol
Bulgarie	dépend de l'accord
Costa Rica	espagnol
Croatie	croate, anglais
Chypre	grec et anglais
République dominicaine	espagnol
Estonie	estonien, anglais
Finlande	finnois ou suédois (les demandes dans d'autres langues peuvent être exécutées si cela peut par ailleurs se faire. L'acceptation pourrait être possible par décret). Anglais également accepté en pratique.
France	français, anglais
Géorgie	géorgien, anglais, français, espagnol
Allemagne	allemand
Hongrie	anglais
Japon	japonais
Lettonie	letton
Lituanie	lituanien, anglais, russe
Moldova	moldave, anglais
Monténégro	monténégrin, anglais, français
Pays-Bas	néerlandais, français, anglais, allemand
Norvège	anglais, norvégien, suédois, danois
Philippines	anglais
Portugal	portugais (sauf autres dispositions)
Roumanie	roumain, anglais, français
Serbie	serbe, anglais
Slovaquie	slovaque
Slovénie	anglais
Espagne	espagnol
Suisse	allemand, français, italien, anglais
«ex-République yougoslave de Macédoine»	pas de conditions spécifiques. La langue de l'Etat requérant est acceptée.
Turquie	turc, anglais en cas d'urgence
Ukraine	langue de l'Etat requérant, anglais
Royaume-Uni	anglais
États-Unis d'Amérique	anglais

[17] Des accords bi- ou multilatéraux peuvent prévoir des conditions différentes en matière de langue.

3.4 Procédure pour l'envoi/la réception des demandes

En général, la procédure à suivre pour envoyer une demande d'entraide est la suivante :

1. le Procureur ou les services de poursuite responsables d'une enquête préparent la demande d'entraide ;
2. ils l'envoient ensuite à l'autorité centrale pour vérification (et traduction, si nécessaire) ;
3. l'autorité centrale (ministère de la Justice, Service du Procureur) soumet la demande
   - soit à l'autorité centrale du pays requis,
   - soit directement à l'autorité judiciaire requise.

La procédure en cas de réception et d'exécution d'une demande est la suivante :

1. réception de la demande par l'autorité centrale ;
2. examen du respect des conditions formelles et légales (et traduction, si nécessaire) ;
3. transmission au Procureur ou aux services de poursuites compétents pour obtenir une injonction du tribunal ;
4. délivrance d'une injonction du tribunal ;
5. le Procureur ordonne aux services d'exécution de la loi (Service de lutte contre la cybercriminalité) d'obtenir les données ;
6. examen des données obtenues par rapport à la demande d'entraide qui peut comprendre une traduction or le recours à un spécialiste de la langue;
7. transmission à l'Etat requérant par les canaux propres à l'entraide.

Si une demande ne respecte pas les conditions de procédure, le processus peut comporter diverses étapes intermédiaires supplémentaires. Une demande d'entraide peut aussi s'accompagner d'une demande parallèle de conservation des données.

Les réponses laissent à penser qu'il existe un certain nombre de cas de figure :

- entre les pays de l'UE, les demandes peuvent être envoyées directement aux autorités requises (non par le biais des autorités centrales) ;
- Bosnie-Herzégovine, France : utilisation des canaux d'INTERPOL pour les demandes d'entraide.
- Estonie : en cas d'urgence, les demandes sont présentées via les canaux d'Interpol, ou une notice Schengen peut être exécutées avec l'aval du Bureau du Procureur, avant qu'une demande d'entraide formelle soit reçue par le ministère de la Justice ;
- Allemagne : contact préliminaire par un point de contact 24/7 avec des homologues étrangers en vue d'un possible déclenchement d'une enquête au niveau national ;
- Japon : si la demande n'est pas basée sur un accord d'entraide mais sur la réciprocité, elle est envoyée par les canaux diplomatiques ;
- Norvège : la demande d'entraide peut être accompagnée d'une décision judiciaire ordonnant que des conditions en vigueur au niveau national doivent être remplies pour obtenir les données ;
- Serbie : contact avec les autorités étrangères pour vérifier si les données peuvent être obtenues sans demande d'entraide formelle ;
- Slovénie : les demandes peuvent être envoyées ou reçues par le Secteur de la coopération policière internationale (IPCS).

Conclusions préliminaires :

- la possibilité de coopérer directement avec des autorités judiciaires étrangères semble sous-utilisée – excepté entre États membres de l'UE. Cette utilisation limitée semble aussi être le cas

pour les Parties au 2e Protocole additionnel à la Convention relative à l'entraide en matière pénale (STE 182) du Conseil de l'Europe ;

- il peut être intéressant d'examiner la possibilité d'une coopération directe dans un Protocole à la Convention de Budapest sur la cybercriminalité ;

- il peut être utile d'envisager de simplifier les obligations légales et formelles dans un Protocole à la Convention de Budapest tout en conservant les sauvegardes et conditions pour les mesures coercitives ;

- les contacts avec des homologues dans la Partie requise sont encouragés en vue de limiter les procédures nationales dans cet Etat.

3.5 Problèmes rencontrés

Les réponses font ressortir les problèmes suivants rencontrés dans le processus de demande d'entraide :

- temps, charge de travail et complexité des procédures requises pour préparer ou exécuter une demande d'entraide (Albanie, Belgique, Chypre, Finlande, France, Italie, Japon, République de Moldova, Philippines, Roumanie, Serbie, Slovénie, Turquie et États-Unis).

- Temps de réponse (6 – 24 mois) aux demandes en général ou par rapport à certains pays (Albanie, Australie, Belgique, Croatie, République dominicaine, Finlande, Lettonie, Norvège, Roumanie et Serbie).

- Temps pris pour communiquer des données sur l'abonné (Allemagne).

- Refus de certains pays de coopérer pour des infractions « vénielles » (Autriche, Costa Rica, France, Roumanie).

- Refus de coopérer ou pas de réponse par certains pays (Bulgarie, Estonie, Slovénie).

- Problème de coopération avec des points de contact 24/7 (Turquie).

- Pas d'accusé de réception des demandes d'entraide ou de confirmation que des données ont été conservées (Suisse, Royaume-Uni).

- Critères non clairs pour des demandes « urgentes » (Suisse).

- Problème langue, qualité de la traduction, terminologie utilisée (Turquie, Royaume-Uni).

- Demandes reçues pour un périmètre trop large, pour un gros volume de données (Pays-Bas, Espagne).

- Différences entre les systèmes légaux, par exemple pour les pouvoirs d'enquête (Albanie, Moldova, Norvège, Roumanie, Serbie, Ukraine).

- Restrictions légales (protection des données) (Albanie, France, Moldova, Serbie).

- Refus de coopération par un Etat étranger sans demande d'entraide. Or, la demande d'entraide exige des informations et preuves suffisantes, qui ne peuvent être obtenues sans coopération par l'Etat étranger (cercle vicieux) (Arménie, Belgique).

- Il est possible que la demande ne respecte pas le seuil légal ou les exigences formelles de l'Etat requis ou qu'elle ne soit pas complète ou encore que seuil/standard requis soit trop élevé (Australie, Autriche, Finlande, Allemagne, Lituanie, Slovaquie, États-Unis).

- Inadéquation des lois (États-Unis).

- Principe de la double incrimination non respecté (Serbie).

- Demande d'entraide non précédée d'une demande de conservation pour s'assurer que les données sont encore disponibles (Australie, Slovaquie).

- Données non conservées dans l'Etat étranger en dépit d'une demande de conservation (Estonie).

- Données ne sont plus disponibles dans l'Etat étranger ou dans l'Etat requérant (Géorgie, Italie, Norvège, Portugal, Roumanie, Suisse).

- Différentes politiques suivies par les fournisseurs pour rendre les données disponibles (Belgique).

- Personne de contact en cas d'urgence ou autorité compétente dans l'Etat étranger inconnues (Bosnie-Herzégovine, Géorgie, et Pays-Bas).

- Difficulté pour identifier les préoccupations de l'autorité, par exemple fournisseur d'hébergement sur le web (Norvège).

- Demandes trop nombreuses, d'où une surcharge (Chypre, États-Unis).

- Compétences techniques et compréhension de la preuve électronique limitées dans l'Etat requis (États-Unis).

- Pouvoir limité de la police judiciaire (Portugal).

- Seuil de la « cause probable ».

Conclusions préliminaires :

- Contact direct avec les autorités étrangères pour demander conseil sur les exigences à respecter avant d'envoyer une demande d'entraide (Australie) ou de faire une demande de conservation ou d'entamer une enquête parallèle (Norvège).

3.6 Tableaux concernant les questions 2.1 – 2.5

3.6.1 Conditions et motifs de refus (Questions 2.1 – 2.3)

2.1 Critères à respecter pour exécuter une demande d'entraide

Lorsque vous recevez une demande concernant des données informatiques stockées, quels critères formels, juridiques ou autres devez-vous respecter pour pouvoir exécuter la demande ? Veuillez donner des exemples, y compris sur des demandes que vous avez dû rejeter.

Quel est le fondement juridique qui vous permet d'exécuter ce type de demande ? Veuillez joindre en annexe le texte des dispositions légales pertinentes.

2.2 Motifs de refus de coopérer

Les Parties qui reçoivent une demande peuvent refuser de coopérer dans certaines circonstances (voir par exemple les articles 25.4 et 27.4 de la Convention de Budapest). Veuillez énumérer les motifs de refus et donner des exemples de demandes que vous avez refusé d'exécuter.

2.3 Langue de la demande

Lorsque vous recevez une demande, quelles sont vos exigences concernant la langue ?

Quelle est l'ampleur du problème de la traduction depuis et vers les langues étrangères sur les plans du temps, de l'argent et de la qualité ? Quelles solutions proposeriez-vous pour y remédier ?

Pays	**Critères à respecter (Q 2.1)**	**Motifs de refus de coopérer (Q 2.2)**	**Langue de la demande (Q 2.3)**
Albanie	– Contenu de la demande : description des actions à entreprendre ; motifs de la demande ; autres données pertinentes. – Respect de la procédure applicable, y compris l'exigence d'une injonction	– Motifs spécifiés par la Convention Cybercriminalité appliqués aux demandes émanant de Parties à la Convention. – Motifs de refus des demandes émanant d'États non-Parties :	Requis : albanais. Accepté : anglais. *Problèmes et solutions* : coût financier et temps nécessaire pour traduire les demandes (en particulier dans les langues nationales).

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	judiciaire.	L'action demandée est expressément interdite par la loi ou contrevient aux principes fondamentaux de l'Etat de droit en Albanie ; Des considérations concernant la race, la religion, le sexe, la nationalité, la langue, les opinions politiques ou le statut social peuvent nuire à la performance du processus [à clarifier] ; Pas de garanties suffisantes contre une ingérence excessive d'une personne citée (témoin, expert, accusé) ; Pas de garantie de réciprocité donnée par l'Etat requérant.	Suggestion : privilégier l'anglais dans les communications relatives aux demandes d'entraide.
Arménie	Chapitre 54 du code de procédure pénale	Motifs de refus décrits dans le CPP arménien. De plus, il ne peut être donné suite à une demande si les informations sont insuffisantes ou les informations demandées non disponibles.	anglais, russe, arménien
Australie	– Respect des conditions permettant à l'AG (Attorney-General) d'autoriser un service répressif à demander une injonction d'obtention de communications stockées (la demande doit émaner de l'autorité étrangère pour que l'AG prenne les dispositions nécessaires à l'accès aux communications stockées ; l'enquête a déjà démarré dans le pays requérant ; l'infraction est punissable d'une sanction maximum – pour le plafond, voir législation - ; il y a des motifs raisonnables de penser que le détenteur détient des données stockées pertinentes ; – L'autorité judiciaire peut ensuite délivrer un	Motifs *obligatoires* (appliqués par l'AG) : – La demande concerne un délit politique ou infraction liée ; une infraction purement militaire ; – il y a des motifs substantiels de croire que la demande a été introduite pour des raisons de race, de sexe, d'orientation sexuelle, de religion, de nationalité ou d'opinions politiques de la personne concernée ; – il y a des motifs substantiels de croire que, s'il est fait droit à la demande, la personne concernée court le risque d'être torturée ; – faire droit à la demande porterait préjudice à la souveraineté, à la sécurité ou aux intérêts nationaux du pays ou à d'autres intérêts essentiels ;	Exigé : anglais. *Problèmes* Qualité variable des traductions dans les demandes entrantes, qui peuvent retarder leur traitement (par exemple nécessité de demander des éclaircissements aux autorités étrangères). *Solutions* Conserver une liste de traducteurs professionnels efficients pour les demandes sortantes. Toutes les demandes d'entraide devraient être traduites par des

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	mandat à l'officier de police à certaines conditions (le processus de demande a été rempli ; il y a des motifs raisonnables de suspecter qu'un support spécifique contient les données stockées recherchées ; les informations susceptibles d'être obtenues par cet accès aux données devraient aider l'enquête entamée par des autorités étrangères).	– la demande concerne une infraction pour laquelle le pays étranger peut infliger la peine de morts (exceptions prévues). Motifs *discrétionnaires* : – le principe de la « double incrimination » n'est pas respecté ; – 'Ne bis in idem' et autres : la demande concerne une personne qui a été acquittée, graciée ou a purgé sa peine ; – l'entraide pourrait porter atteinte à des enquêtes ou procédures criminelles dans le pays requis ; – l'entraide pourrait porter atteinte à la sécurité d'une personne ; – l'entraide imposerait une charge excessive sur les ressources du pays requis ; – toute autre situation où il est approprié de refuser l'entraide.	traducteurs de niveau professionnel.
Autriche	– Respect de la procédure applicable ; – Adjonction en annexe à la demande de l'original ou de la copie certifiée de l'injonction de l'autorité pertinente (en l'absence d'une injonction de tribunal, déclaration par l'autorité étrangère que les conditions exigées en droit interne du pays requérant sont remplies).	Les motifs dépendent des faits de l'affaire et des informations demandées, et incluent un certain seuil de gravité de l'infraction. Ainsi, une demande pour des données relatives au contenu dans un cas de simple fraude sera refusée.	Accepté : allemand, anglais, ou français. Des accords bilatéraux supplémentaires peuvent prévoir des décharges mutuelles de responsabilité concernant les traductions. Suggestions : – il est souhaitable de supprimer les conditions de traduction (une traduction de meilleure qualité peut être obtenue dans l'Etat requis) ;

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
			– Il conviendrait peut être d'éviter les programmes de traduction automatique.
Azerbaïdjan	Les critères sont ceux des accords internationaux y compris la Convention sur la cybercriminalité.	L'exécution de la demande est incompatible avec le droit national	Accepté : anglais, turque ou russe
Belgique	La coopération judiciaire est principalement régie par la Loi du 9 décembre 2004. La demande d'entraide doit être en conformité avec l'instrument juridique international sur lequel elle se base. La législation nationale ne prévoit pas de conditions supplémentaires. En cas de demande, – un Procureur peut obtenir d'un fournisseur de services des renseignements concernant des abonnés sans avoir besoin de l'autorisation d'un juge d'instruction (Art. 46bis Code d'instruction criminelle), – un juge d'instruction peut obtenir des données d'appel ou de localisation directement auprès d'un fournisseur.	Seuls les motifs de refus prévus dans l'instrument pertinent sont applicables. Toutefois, l'exécution d'une demande peut être retardée si ceci va dans l'intérêt d'une enquête en cours en Belgique.	Les demandes reçues en anglais sont acceptées mais doivent être traduites dans les trois langues officielles de la Belgique. Globalement, la question des traductions est un gros problème, du fait des coûts et aussi du nombre limité de traducteurs qualifiés. Une base de données dynamique ou un glossaire contenant les termes clés serait utile. Une autre possibilité sera que l'anglais serve de langue commune pour les procédures.
Bosnie-Herzégovine	– *Contenu* de la demande : nom de l'autorité étrangère et, si possible, de l'autorité requise ; base légale ; identification de l'infraction pénale et du suspect ; description factuelle de l'infraction ; préjudice causé ; mesures qui devraient être prises ; autres données pertinentes. – Respect de la procédure applicable, en particulier des conditions applicables pour	Motifs *discrétionnaires* : – l'entraide peut être refusée sur la base d'une réciprocité factuelle pour ce qui concerne un pays particulier. Motifs *obligatoires* : a) si l'exécution de la demande porterait préjudice à l'ordre juridique de la Bosnie-Herzégovine, à sa souveraineté ou à sa sécurité ;	Exigé : l'une des langues de Bosnie-Herzégovine (bosniaque, croate ainsi que Serbe), traduction certifiée par un traducteur juré. Toléré : (canaux d'Interpol) anglais. *Problèmes et solutions* : n/a.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	l'obtention d'une injonction judiciaire à l'encontre d'un FSI (soupçon de commission d'une infraction ; les informations peuvent server de preuve ou autrement dans des procédures pénales)	b) si la demande concerne une infraction considérée comme un délit politique ou une infraction liée à un délit politique ; c) si la demande concerne une infraction pénale militaire ; d) si la personne accusée de l'infraction pénale visée a été acquittée pour des motifs de droit matériel ou si la procédure à son encontre s'est terminée par un non-lieu, ou si elle a été graciée ou a exécuté sa peine ou que celle-ci ne peut être exécute en vertu du droit du pays où le verdict a été prononcé ; e) si des procédures pénales sont en cours contre la personne en Bosnie-Herzégovine pour la même infraction pénale, à moins que l'exécution de la demande n'entraine une décision de libération de l'accusé ; f) si les dispositions concernant la prescription empêcheraient des poursuites pénales ou l'exécution d'une sanction en vertu du droit national. *Problèmes pratiques* : demande trop succincte ; impossibilité d'établir l'infraction pénale.	
Bulgarie	– *Contenu* de la demande : informations sur l'autorité requérante ; objet et raison de la demande ; nom et nationalité de la personne concernée ; nom et adresse de la personne à laquelle des documents juridiques doivent être présentés ; si nécessaire, chefs d'accusation et résumé des faits pertinents.	– si l'exécution de la demande risqué de menacer la souveraineté, la sécurité nationale, l'ordre public et d'autres intérêts protégés par la loi ; – si l'exécution de la demande risqué de faire obstacle à des actes d'enquête ou au recueil de données pour le déclenchement de poursuites pénales ; – si l'exécution de la demande risque de mettre	En fonction des accords internationaux applicables entre les pays requérant et requis. *Problèmes* La traduction des demandes prend trop de temps et coûte trop cher.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	– Existence d'un fondement juridique (accord international, ou en l'absence d'un tel accord fondement sur le principe de la réciprocité)	en danger la vie d'une personne physique ; – si les informations demandées ne correspondent pas à l'objectif de la demande ; – Si les informations demandées concernent un délit véniel.	
Costa Rica	Respect des conditions établies dans les instruments internationaux applicables. *Remarque*. Les autorités nationales coopèrent avec l'Etat requérant, avec ou sans le soutien d'un accord international.	Si la demande implique des procédures ou des requêtes contraires aux droits fondamentaux et garanties que la Constitution et les lois donnent au peuple.	Exigé : espagnol. *Problèmes* – Temps nécessaire pour traduire les demandes ; – Ressources humaines et financières exigées.
Croatie	– *Forme* de la demande : par écrit, ou sous forme électronique laissant un enregistrement écrit, à condition que son authenticité puisse être établie et que la méthode d'envoi soit expliquée dans la demande ; – Contenu de la demande : Lieu d'émission ; nom de l'autorité étrangère compétente qui envoie la demande ; base légale de cette dernière ; description et justification de la demande ; intitulé légal, courte description factuelle et juridique de l'infraction* ; informations sur la personne concernée (données, nationalités, position dans la procédure) ; si pertinent, type d'injonction judiciaire transmise. *Exception : lorsque la demande concerne la notification de décisions judiciaires et autres actes similaires.	Motifs *discrétionnaires* : – si la demande concerne un délit politique ou une infraction liée à un délit politique (hormis les crimes internationaux) ; une infraction fiscal ; – si l'exécution de la demande porterait préjudice à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels de l'Etat ; – s'il est présumé que la personne dont l'extradition est demandée serait poursuivie ou punie pour des motifs liés à la race, à la religion, à la citoyenneté, à l'affiliation à un groupe social précis, ou pour ses convictions politiques ; – si l'infraction pénale est vénielle. Motifs *obligatoires* : – 'Ne bis in idem' et autres : affaires pour lesquelles en Croatie il y aurait acquittement sur une base de droit matériel, interruption de	Exigé : croate. Accepté : anglais ("s'il n'est pas possible de la rédiger en croate, une traduction en anglais sera acceptée"). Les traductions doivent être jurées. *Problèmes et solutions* : La traduction, en particulier le temps nécessaire pour traduire les demandes, sape l'efficacité des services répressifs. Suggestion : il conviendrait de privilégier les communications de demande d'entraide par le biais des points de contact.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
		la procédure, sursis de la sentence, sanction ayant été exécutée ou qui ne peut pas être exécutée au titre du droit étranger applicable*. – si des poursuites pénales pour la même infraction sont en course en Croatie (exception : si l'exécution de la demande d'entraide peut aboutir à la mise en liberté de l'accusé) ; – si la prescription interdit les poursuites ou sanctions pénales au titre du droit national*. – *Exception : si le jugement final a été révisé dans l'Etat requérant.	
Chypre	Une demande formelle écrite d'entraide doit être adressée à l'Autorité central (ministère de la Justice & de l'Ordre public) ; elle doit contenir tous les éléments pour son exécution (résumé des faits, dispositions juridiques pertinentes et actions demandées).	Motifs énumérés aux articles 25.4 et 27.4 Convention de Budapest. Refus si les éléments essentiels d'une demande écrite ne sont pas respectés. Condition préalable : l'infraction objet de l'enquête dans l'Etat requérant doit être punissable d'une peine d'emprisonnement pouvant aller jusqu'à 5 ans.	anglais et grec. Problèmes : les traductions retardent les réponses. Solution : utiliser l'anglais.
République dominicaine	Les demandes doivent toujours être envoyées par le biais du ministère public.	N/A	La demande doit être envoyée en espagnol.
Estonie	*Contenu de la* demande : nom de l'autorité requérante ; contenu [mesures demandées] ; détails relatifs à la personne concernée ; faits et évaluation juridique de l'infraction pénale.	– la demande peut mettre en danger la sécurité, l'ordre public ou d'autres intérêts essentiels de l'Etat ; – la demande est contraire aux principes généraux du droit national ; – il y a lieu de penser que la demande concerne des chefs d'accusation/sanctions fondés sur des motifs discriminatoires (race, nationalité, religion etc.) ; – Remarque : le caractère politique de l'infraction n'est pas un motif de refus en ce qui concerne	Exigé : estonien ou anglais. *Problèmes* La traduction de tous les documents entraîne une charge de travail et des coûts supplémentaires.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
		les pays de l'UE (sauf exceptions).	
Finlande	– Lorsque des mesures coercitives sont nécessaires, respect des conditions du droit national sur ce point ; – *Forme* de la demande : par écrit, sous forme d'enregistrement, oralement ou sous forme électronique ; – *Contenu* de la demande : identification de l'autorité requérante, et, si nécessaire, des autorités compétentes en matière de poursuites et d'enquêtes ; objet et raison de la demande ; informations sur la personne concernée ; description de l'infraction et du droit applicable ; faits et comportement criminel ; description des preuves recherchées et des informations liées ; indemnités et dépens des témoins ou experts intervenants. – lorsqu'une notification d'un document judiciaire est requise, le document à notifier doit être joint. Forme et contenu : la demande peut toutefois être exécutée si les problèmes de forme et de contenu ne sont pas de nature à faire obstacle à l'exécution.	Motifs *obligatoires* – Si l'exécution de la demande porterait atteinte à la souveraineté, à la sécurité ou à d'autres intérêts essentiels de l'Etat ; – si l'exécution de la demande serait contraire aux principes des droits de l'homme, aux libertés fondamentales ou à l'*ordre public*. Motifs *discrétionnaires* – si l'infraction est politique ou purement militaire ; – si l'auteur de l'infraction ne peut plus être poursuivi, en droit national (prescription, grâce ou autres) – si une enquête, des poursuites ou des procédures pénales ont été entamées dans un Etat (Finlande ou autre) concernant l'infraction ; – si une enquête, des poursuites ou des sanctions ou autres ont été abandonnées dans un Etat (Finlande ou autre) ; – si l'auteur de l'infraction a été condamné ou acquitté pour l'infraction dans un Etat (Finlande ou autre) ; – si l'exécution de la demande ferait peser une charge déraisonnable sur les ressources disponibles. Indépendamment des dispositions du droit général sur l'entraide, celle-ci sera fournie en vertu des conventions internationales ou autres instruments	Exigé : finnois ou suédois Exceptions : une autre langue peut être acceptée, lorsque cela est autorisé par décret ou, plus généralement, lorsque cela est possible. *Problèmes et solutions* n/a.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
		auxquels la Finlande est partie. La Finlande étant partie à la Convention sur la cybercriminalité, cela crée en soi des obligations et des responsabilités ou définit les motifs de refus.	
France	– Respect de la procédure applicable en droit national, notamment pour ce qui est de l'émission d'une injonction judiciaire.	– si la demande demande la transmission directe de données, alors que le droit national exige pour cela qu'une injonction judiciaire soit rendue ; – si la demande concerne une infraction vénielle ; – si la demande n'est pas suffisamment justifiée au regard des contraintes qu'elle entraîne. – Pour ce qui est des demandes de pays de l'UE (voir art. 695-9-41 CPP), l'exécution de la demande ne peut être refusée que dans les cas suivants : – si cela porterait préjudice aux intérêts fondamentaux de la nation en matière de sécurité nationale ; – si cela porterait préjudice à une enquête criminelle ou mettrait en danger la sécurité d'une personne ; – si cela serait manifestement disproportionné ou sans objet au regard du résultat visé tel que mentionné dans la demande.	Accepté : français et anglais. *Problèmes* En tant qu'Etat requis, pas de problème spécifique concernant les demandes traduites par l'unité nationale pour Europol ou Interpol. En tant qu'Etat requérant, la traduction ne peut pas toujours être assurée par le personnel qui ne maîtrise pas l'anglais. Suggestion : privilégier davantage de formation en anglais pour le personnel amené à traiter des questions de coopération internationale.
Géorgie	– *Contenu de la* demande : indication des faits, qualification légale de l'affaire, but et nécessité de la demande ; chaque fois que possible, description détaillée permettant d'identifier la personne concernée ; – lorsque la demande concerne une perquisition et saisie, principe de la double	– l'exécution de la demande menace la souveraineté, la sécurité publique ou d'autres intérêts vitaux de l'Etat ; – elle est incompatible avec le droit interne ; – elle concerne un délit politique ou une infraction liée à un délit politique (sous réserve d'exceptions) ou une infraction purement	Pas de conditions spécifiques. En pratique : essentiellement anglais, français ou espagnol. *Problèmes et solutions* Temps nécessaire pour traduire les demandes.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	incrimination ; l'infraction peut déboucher sur une extradition ; respect d'autres dispositions du droit interne.	militaire ; – elle met en danger les droits de l'homme et les libertés fondamentales ; – elle viole le principe ne bis in idem	Suggestion : privilégier l'anglais et le français.
Allemagne	– La demande doit être émise par une autorité judiciaire ; – une injonction judiciaire ou équivalent doit être émise par l'Etat requérant ; – les faits doivent être décrits dans la demande ; – le principe de la double incrimination doit être respecté ; – la demande doit être traduite.	– la demande ne respecte pas les conditions prévues par le droit national ; – les preuves sont prévues pour être utilisées dans des procédures judiciaires pouvant se solder par une condamnation à mort, sans garantie de l'Etat requérant qu'il n'appliquera pas cette sanction.	Exigé : allemand. *Problèmes* Le temps nécessaire pour traduire les demandes retarde parfois l'exécution de ces dernières.
Hongrie	Pour répondre à une demande, la double incrimination est une condition.	Si la demande : – est contraire au droit hongrois – menace la sécurité et l'ordre public en Hongrie – concerne des délits politiques ou militaires.	anglais. Principal problème : délais de traduction. Les demandes devraient être envoyées à la Hongrie en anglais.
Islande	Limite de temps : aucun. Néanmoins selon la loi islandaise, les entreprises doivent supprimées les données stockées (données informatiques/IP dans les 6 mois. Documentation : Description de la procédure juridique en cours, informations sur ladisposition concernée, des dispositions applicables dans l'État requérant, informations sur les mesures sont requises, information sur la personne ou l'entreprise la demande concernée. Exigences spéciales peuvent être nécessaires lorsque certaines actions sont réclamées.	Non-respect du principe de double incrimination. La demande concerne une infraction politique ou militaire. Exécution de la demande est susceptible de porter atteinte à la souveraineté, la sécurité ou l'ordre public de l'État. Motifs raisonnables de croire que les procédures sont fondées sur des motifs liés à la race, nationalité, religion, convictions politiques, etc..	Islandais, anglais novegien, danois ou suédois. Les traducteurs islandais etant peu nombreux en dehors de l'Islande, il est Généralement mieux de recevoir les demandes dans un bon niveau d'anglais plutôt que dans un islandais à niveau faible. Les traductions en islandais sont souvent d'un faible niveau et quelques fois incompréhensibles.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	Double incrimination : Oui. Cependant, la double incrimination est seulement requise au sujet de délits politiques lorsque la requête provient du Danemark, de Finlande, de Norvège ou de Suède		
Japon	Les conditions à remplir sont prévues par les accords internationaux applicables, en particulier la Convention sur la cybercriminalité. Lorsque la demande n'est pas basée sur un traité, les conditions suivantes s'appliquent : – assurance de la réciprocité ; – principe de la double incrimination ; – caractère non politique de l'infraction ; – démonstration par écrit que les preuves sont essentielles à l'enquête (pour les demandes de récupération de preuves ou de témoignages).	Les motifs de refus concernent le non-respect des conditions suivantes : – assurance de la réciprocité ; – principe de la double incrimination ; – caractère non politique de l'infraction ; – démonstration par écrit que les preuves sont essentielles à l'enquête (pour les demandes de récupération de preuves ou de témoignages). Motifs supplémentaires : ceux prévus dans l'accord international utilisé comme base juridique.	Exigé : japonais. *Problèmes* En tant qu'Etat requérant : temps nécessaire et nombre limité de traducteurs professionnels ayant l'expertise requise.
Lettonie	– Décision de l'autorité nationale compétente sur l'admissibilité de l'action procédurale à exécuter ; – Consentement (avant le procès) des autorités compétentes (Bureau du Procureur général ; Police d'Etat) pour exécuter la demande ; – Adjonction en annexe d'informations suffisantes et de la documentation exigée (injonction d'un tribunal pour la divulgation de données relatives au contenu)	– la demande concerne un délit politique (exceptions : terrorisme, financement du terrorisme) ; – l'exécution de la demande peut porter atteinte à la souveraineté, à la sécurité, à l'ordre social ou à d'autres intérêts fondamentaux de l'Etat ; – les informations sont insuffisantes et qu'il n'est pas possible de les compléter.	Exigé : letton (à moins d'autre accord avec l'Etat requérant). Problèmes : le temps nécessaire pour traduire les demandes. Solution : établir une procédure différente pour la langue à utiliser, par des contacts directs et des accords.
Lituanie	(Voir article 29 de la Convention de Budapest) Contenu de la demande : identification de	– Manque des informations prévues à l'article 29 de la Convention de Budapest ou les	Langues préférées : lituanien, anglais ou russe.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	l'autorité requérante, de l'infraction concernée, bref résumé des faits, données à conserver et lien avec l'affaire, informations identifiant le détenteur des données ou la localisation du système informatique, nécessité de la conservation, intention de soumettre une demande d'entraide pour la perquisition, la saisie, la divulgation et les actions connexes. Pas de motifs de refus.	informations fournies sont à l'évidence inexactes et ne peuvent être complétées ou rectifiées ; – la demande contrevient aux principes légaux du droit national (constitutionnel) ou du droit international (ne bis in idem, non-discrimination, impartialité, procès équitable etc.) ; – il y a des motifs raisonnables de penser que l'exécution de la demande risque de porter atteinte aux intérêts fondamentaux de l'Etat (souveraineté, sécurité, ordre public, risque pour des vies humaines etc.) ; – il y a des motifs raisonnables de penser qu'au moment de la divulgation, l'infraction sur laquelle se base la demande n'est pas considérée comme un délit dans le droit lituanien.	*Problèmes* Pas de problèmes majeurs pour les demandes rédigées en anglais ou russe. Pour d'autres langues, cela entraîne des retards et des coûts.
Moldova	– *Forme* de la demande : par écrit ; – Contenu de la demande : identification de l'autorité requérante ; nom et adresse (si disponibles) de l'autorité destinataire ; description de l'affaire, avec les faits, les dispositions applicables du Code pénal moldave, les préjudices causés ; informations sur la personne qui fait la demande ; objet de la demande et données nécessaires pour l'exécuter, notamment les circonstances, listes de documents, preuves demandées etc. ; la date à laquelle on souhaite obtenir la réponse ; tous les actes procéduraux nécessaires en pièces jointes ;	Motifs *discrétionnaires* : – la demande concerne un délit politique (exception : crimes internationaux en vertu du Statut de la CPI) ou un délit purement militaire ; – l'exécution de la demande risque de porter atteinte à la souveraineté, à la sécurité ou à l'ordre public de l'Etat ; – il y a des motifs raisonnables d'estimer que les procédures sont fondées par des motifs de race, de religion, de nationalité, de convictions politiques etc. ; – la personne concernée n'aura pas droit à un procès équitable ;	Exigé : moldave. Toléré : anglais. note : moldave ou autres langues (en vertu des accords internationaux applicables). *Problèmes et solutions* : coût et temps supplémentaires pour traduire les demandes (en particulier pour les langues nationales). Suggestion : privilégier l'anglais dans les communications en matière de demandes d'entraide.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	la signature et le cachet officiel de l'autorité requérante.	– l'Etat requérant punit l'infraction de la peine capitale et ne donne pas de garantie que cette peine ne sera pas prononcée ou appliquée ; – en cas de non-respect du principe de double incrimination ou d'absence de responsabilité pénale dans le droit interne.	
Monténégro	*Contenu de la* demande : nom et siège de l'autorité expéditrice de la demande ; nom de l'autorité requise ou au minimum indication du pays et de l'autorité judiciaire compétente ; base légale de la demande ; forme et justification de l'entraide requise ; qualification juridique de l'infraction et résumé des faits* ; le cas échéant, type d'injonction du tribunal transmise. *Exception : lorsque la demande concerne la notification de décisions de tribunal et autres actes similaires	[à clarifier]	Exigé : la langue officielle. Toléré : langues officielles du Conseil de l'Europe (anglais, français). *Problèmes et solutions* : pas de problèmes spécifiques, étant donné que les demandes sont habituellement traduites en anglais.
Pays-Bas	– Existence d'une affaire pénale (autrement dit une procédure pénale a été intentée à l'étranger) – le comportement constitue une infraction dans le droit de l'Etat requérant ; – le comportement constitue une infraction dans le droit de l'Etat requis ; – l'infraction figure sur la liste de celles pour lesquelles une garde-à-vue préventive est autorisée.	Motifs *obligatoires* – la demande concerne un comportement non poursuivi au niveau national ; – le principe de la double incrimination n'est pas respecté Motifs *soumis à aval* du MJ : – la demande fait craindre un procès discriminatoire ; – la demande concerne un délit politique ou fiscal ; – le MJ a donné instruction de ne pas exécuter la	(uniquement applicable aux demandes basées sur la Convention des Nations Unies contre le Trafic illicite de stupéfiants et de substances psychotropes). Exigé : néerlandais, français, anglais ou allemand. *Problèmes* n/a.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
		demande.	
Norvège	– Principe de double incrimination ; – (exigence pratique) identification de la personne juridique/morale détentrice des données ; – concernant les journaux d'IP, respect du délai de conservation actuellement en vigueur (21 jours).	– non-respect du principe de la double incrimination ; – la demande concerne une affaire de diffamation et ne donne pas suffisamment d'éclaircissements concernant l'infraction alléguée ; – l'exécution de la demande créerait des difficultés pratiques (par exemple, trop de témoins à entendre).	Privilégié : anglais, norvégien, suédois ou danois. *Problèmes* – capacité limitée de traducteurs en interne ; – nécessité, en tant qu'Etat requis, de traduire les principaux faits et documents en norvégien.
Philippines	Le Ministère de la Justice traite toutes les communications relatives à l'entraide. Etat requis Evaluation Exécution des demandes par le Ministère de la Justice ou d'autres autorités compétentes Sur exécution, documents/preuves demandés transmis au Ministère de la Justice Le Ministère de la Justice transmet les documents/preuves recherchés, transmet à l'Etat requérant au travers de la voie diplomatique Etat requérant : Les forces de l'ordre et le ministère public soumettent les demandes au Ministère de la Justice Evaluation En cas d'information insuffisante, coordonne avec les agences/ autorités pour compléter/se	Les motifs de refus sont différents d'un accord bilatéral à l'autre en matière d'entraide. Ainsi, celui conclu avec l'Inde prévoit qu'une partie peut refuser l'entraide pour l'un des motifs suivants: a. l'exécution de la demande porterait atteinte à la souveraineté, à la sécurité, à l'ordre public ou à tout autre intérêt essential de la nation, ou à la sécurité d'une personne ; b. elle serait contraire au droit interne de la Partie requise ; c. si la demande a pour objet la mise sous séquestre, la saisie ou la confiscation de biens ou d'instruments d'une activité qui, si elle avait eu lieu dans la juridiction de la Partie requise, n'aurait pas pu donner lieu à une injonction de confiscation ; et d. si elle concerne une infraction pour laquelle la personne mise en cause a été finalement acquittée ou graciée. En tant qu'Etat requérant : compléxité du système	L'utilisation de l'anglais, en tant que langue acceptée partout, est pratique pour les parties.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	conformer aux conditions requises, lorsque la demande est urgente, le Ministère de la Justice informe le CA de l'Etat requis de la demande future dès que les conditions sont remplies, le Ministre de la Justice transmet la demande au CA de l'Etat requis	En tant qu'Etat requis : lois restrictives et différentes interprétations jurisprudentielles par la cours	
Portugal	Respect des conditions prévues dans le droit national pour les perquisitions, la saisie et la divulgation de données, notamment émission d'une injonction par l'autorité judiciaire compétente (sauf s'il en est disposé autrement).	Motifs *obligatoires* : – la procédure ne respecte pas la CEDH ; – la demande fait craindre une discrimination (du fait de la race, religion, sexe, nationalité, langue, convictions politiques d'une personne etc.) ; – la demande prévoit des procédures devant un tribunal d'exception ou l'application d'une sentence dans un contexte de ce type ; – l'infraction est punissable de la peine de mort, ou il y a atteinte irréversible à l'intégrité de la personne ; – l'infraction est punissable d'une peine à vie ou indéfinie ; – la demande concerne un délit politique ou purement militaire.	Exigé : portugais (sauf autres dispositions prévues dans un accord international). *Problèmes* Gros problèmes dus : – au temps et aux coûts entraînés ; – à la difficulté de trouver des traducteurs compétents, en particulier pour des langues rares.
Roumanie	– Contenu de la demande : nom de l'autorité judiciaire requérante et requise ; objet et motifs de la demande ; classification juridique des actes ; informations permettant d'identifier la personne concernée (accusé, défendeur, témoin, expert etc.) ; documents à l'appui, certifiés par l'autorité requérante	– l'exécution porterait atteint à la souveraineté, à la sécurité, à l'ordre public et autre intérêt essentiel de l'État tel que défini par la constitution ; – les poursuites pénales ont déjà eu lieu pour le même acte et (a) un jugement définitif a été rendu pour l'acquittement ou le non-lieu dans le	Accepté : roumain, anglais ou français. *Problèmes* – Ressources financières nécessaires pour traduire les nombreuses demandes et documents joints – Mauvaise qualité de la traduction,

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	– respect des obligations relatives à la transmission directe, au besoin, ou applicables à toute autre modalité de transmission ; – existence d'un fondement juridique (accord international), ou d'une assurance écrite de réciprocité de la part de l'autorité compétente de l'État requérant (sous réserve d'exceptions).	procès ; ou (b) la sanction imposée dans la sentence définitive a été purgée ou fait l'objet d'une grâce ou d'une amnistie. (Exception : si la demande envisage de porter révision de la décision finale – aux conditions établies par le droit national –, ou si un traité applicable fixe des conditions plus favorables concernant le principe de « ne bis in idem »). – Motifs applicables aux affaires d'extradition.	qui entraîne de devoir faire retraduire le tout, avec des retards et des frais supplémentaires.
Serbie	– Contenu de la demande : fondement juridique ; description des actions liées à la demande ; justification de la demande, toutes données pertinentes. – Respect de la procédure applicable, en particulier des conditions pour l'émission d'une injonction de tribunal (obligatoire pour les demandes relatives à une interception ou à une collecte de données). – Principe de la double incrimination (l'infraction doit être incriminée dans le droit national). – La procédure pénale dans le droit national ne doit pas être entièrement terminée. – Les poursuites pénales ne sont pas exclues du faite de la prescription, d'une amnistie ou d'une grâce. – La demande ne se réfère pas à un délit politique ou infractions connexes, ou à des délits militaires. – La demande ne portera pas atteint à la	– Motifs indiqués dans la convention sur la cybercriminalité. – – Motifs prévus au titre du droit national : (non-respect de l'un des critères indiqués en détail pour la question 2.1, voir colonne de gauche)	Exigé : serbe. Toléré : anglais. *Problèmes et solutions* : charges financières et délais pour la traduction des demandes. Suggestion : il serait bon de favoriser l'anglais dans les communications relatives aux demandes d'entraide judiciaire.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	souveraineté, la sécurité, à l'ordre public ou aux autres intérêts essentiels de l'État.		
Slovaquie	La demande d'entraide judiciaire doit être envoyée par l'autorité compétente de l'État requérant et accompagné d'une traduction correcte en slovaque (si la coopération n'est pas basée sur un traité) ou dans toute autre langue (en fonction du régime linguistique géré dans un traité donné). Le contenu d'une demande doit être suffisant pour que celle-ci soit exécutée. Celle-ci devrait inclure, notamment, une référence au traité international (si elle est basée sur un traité), une description de l'infraction, avec la date, le lieu de l'infraction, les informations personnelles concernant les personnes impliquées, la qualification juridique, les dispositions applicables dans le droit de l'État requérant (en particulier pour permettre à l'autorité judiciaire d'évaluer la double incrimination, au besoin), les liens avec la Slovaquie, une description claire de l'action attendue de la part des autorités slovaques (il est extrêmement important d'entrer en communication avec les autorités compétentes à partir du moment où une demande au titre de l'article 29 est transmise à l'État requis).	Motifs énumérés aux articles 25.4 et 27.4 Convention de Budapest.	Langue utilisée basée sur un traité, sinon il est nécessaire de transmettre une traduction dans la langue officielle (slovaque). L'utilisation de l'anglais semble faciliter la coopération. Certains pays prévoient la traduction en slovaque. Jusqu'ici, nous n'avons pas rencontré de difficultés liées à la traduction. Il peut être utile, en particulier en cas d'urgence, d'introduire une nouvelle disposition dans l'éventuel Deuxième Protocole additionnel relative à l'obligation d'accepter une demande au titre de l'article 29 en anglais en cas d'urgence. La même obligation peut être envisagée pour les demandes d'entraide judiciaire (en cas d'urgence seulement).
Slovénie	– description des motifs permettant de suspecter qu'il y a commission d'une	aucune expérience dans ce domaine	Accepté : anglais. (Les autorités nationales traduisent les demandes en

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	infraction ; – respect des obligations relatives à l'émission d'une injonction judiciaire, si nécessaire ; – forme de la demande : par écrit ; – contenu de la demande : informations permettant d'identifier les moyens de communications électroniques ; analyse des motifs raisonnables ; durée pour laquelle les données sont demandées ; autres circonstances justifiant l'exécution de la demande.	motifs existants : – les données requises concernent la sécurité nationale ; – la demande concernant une affaire pour laquelle des poursuites ont déjà été intentées.	slovène).
Espagne	– les conditions juridiques et légales habituelles pour les demandes d'entraide : traduction, description des faits, description de l'infraction etc. ; – émission d'une injonction judiciaire pour obtenir les données de la part des fournisseurs de services sur Internet et autre détenteurs de données ; – la demande doit concerner une infraction grave.	Pas d'informations disponibles.	Exigé : espagnol. (sauf exceptions prévues par des accords bilatéraux). *Problèmes* – Temps et coûts. – Manque de praticiens maîtrisant des langues étrangères.
Suisse	– demande d'une autorité judiciaire répressive ; – présentation suffisante des faits (modus operandi) ; – traduction de la demande (allemand, français, italien) ; – respect de la procédure applicable, y compris pour ce qui est de l'émission d'une	– absence de traduction dans une langue acceptée – pas de compétence de l'autorité requérante pour demander une entraide judiciaire ; – la requête est rétroactive et concerne des données stockées depuis plus de six mois ; – –manque d'information sur les faits (modus operandi).	Exigé : allemand, français, ou italien. En pratique, une version en anglais peut être présentée aux autorités nationales.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	injonction judiciaire ; – l'infraction doit être punissable à la fois dans les pays requérant et requis; – les mesures demandées sont proportionnées aux objectifs indiqués dans la demande.		
«l'ex-République yougoslave de Macédoine»	– *Forme* de la demande : lettre de demande d'entraide – Contenu de la demande : type et localisation des données requises ; infraction pénale concernée ; fondement juridique (code pénal). – Respect de la procédure applicable, y compris pour ce qui est de l'émission d'une injonction de tribunal	– La demande concerne un délit politique ou une infraction connexe, ou une infraction fiscale. – L'exécution de la demande risque de porter atteinte à la souveraineté, la sécurité, à l'ordre public ou d'autres intérêts essentiels de l'État.	pas de conditions spécifiques (la langue nationale de l'autorité requérante est acceptée). Le ministère de la Justice traduit les demandes en macédonien. *Problèmes et solutions* : Coût de la traduction. Suggestion : harmonisation des procédures de demande d'entraide judiciaire, par contenu et par langue.
Turquie	– Condition préalable : existence d'un accord international, ou respect du principe de réciprocité. – Contenu de la demande : identification de l'autorité requérante ; objet et justification de la demande ; type et localisation des données ; identité et nationalité de la personne concernée (quand on les connaît) ; relations entre les données recherchées et un type de crime ; fondement juridique (code pénal) ; description des faits, de	– Les motifs qui sont indiqués dans les instruments internationaux applicables. – L'incapacité des autorités étrangères à donner des garanties, au cas où une saisie ou une confiscation demandée dans la demande d'entraide peuvent entraîner des préjudices financiers – Absence de proportionnalité de la demande – Manque de motifs pour exécuter la demande	Exigé : turc Toléré (urgence) : anglais. *Problèmes et solutions* Suggestion : harmonisation des demandes d'entraide en anglais et langue nationale.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	l'infraction pénale et des sanctions impliquées.		
Ukraine	(MdI) principale condition : accord du Bureau du Procureur général, avec ou en l'absence d'un accord sur l'entraide judiciaire ainsi, en 2012, accord pour l'exécution d'une requête d'une demande émanant du Japon (Ser Sec) – respect de la convention sur la cybercriminalité [lorsqu'elle s'applique], et du droit international ; – respect de la procédure au titre du droit national.	(MdI) Tous motifs prévus par un accord international applicable. En l'absence d'un tel accord, les motifs suivants s'appliquent : – la demande est en contradiction avec les dispositions constitutionnelles et peut porter atteinte à la souveraineté, à la sécurité, à l'ordre public ou à d'autres intérêts de l'État ; – – « ne bis in idem » : la personne concernée déjà été jugée et la décision est entrée en vigueur et a produit ses effets ; – aucun soutien en matière de d'entraide judiciaire par l'État requérant quand elle est demandée ; – la demande concerne une infraction vénielle, qui n'est pas punissable au titre du droit interne ; – il y a des motifs de penser que la demande vise des objectifs discriminatoires, basée sur la race, la couleur, l'opinion politique, la religion, le sexe etc. – l'infraction fait l'objet d'enquêtes préalables ou d'un procès (Serv Sec) : voir ci-dessus.	(MdI) Exigé : comme prévu dans l'instrument international applicable. *Problèmes* : n/a (pas de compétence). (Serv Sec) : comme prévu dans les instruments internationaux, dans la langue du pays requérant ou en anglais. *Problèmes* la traduction est d'autant plus difficile que l'on utilise des termes spécifiques et un langage précis dans les documents judiciaires.
Royaume-Uni	*Contenu de la* demande :	– la demande ne respecte pas les exigences du	Exigé : anglais.

Pays	Critères à respecter (Q 2.1)	Motifs de refus de coopérer (Q 2.2)	Langue de la demande (Q 2.3)
	– les informations sur les sources des numéros de téléphone ; données exactes, heure et lieu de l'incident objet de l'enquête ; détail et rôle des personnes impliquées ; raisons et objectifs de la demande ; raisons pour lesquelles ces objectifs ne peuvent pas être atteints par d'autres moyens ; informations pertinentes devant être analysé pour analyser une éventuelle intrusion dans la vie privée de tiers et moyen de minimiser ceci. – lorsque l'interception des communications est demandée, l'État requérant doit être un État membre de l'UE	statut national ; – l'exécution de la demande n'est pas possible pour des motifs politiques (en d'autres termes, la demande est motivée par des raisons politiques).	*Problèmes et solutions* Toutes les demandes devraient être envoyées en anglais.
États-Unis d'Amérique	– émission d'une injonction du tribunal (national) : (a) une injonction de produire, lorsque les informations demandées ne concernent pas le contenu et que le fournisseur ne souhaite pas les donner volontairement ; (b) une injonction de perquisition, lorsque que les informations demandées concernent le contenu. Conditions : double incrimination (fréquent) ; principe de la « cause probable » – en d'autres termes, l'information donne une base raisonnable de penser qu'un crime a été commis et que le compte concerné contient des preuves de ce crime). – informations montrant la relation entre les données recherchées et l'affaire objet de l'enquête.	– pour n'importe quel motif établi dans la convention sur la cybercriminalité ; – les informations fournies ne sont pas suffisantes pour atteindre le seuil de preuve requis au niveau national permettant d'obtenir des données ; – le comportement n'est pas une infraction pénale en droit national ; – la demande porte atteinte aux intérêts essentiels de l'État (en particulier pour ce qui est de la liberté d'expression.)	Exigé : anglais. Les demandes non formelles peuvent être transmises dans la langue originale. *Problèmes* – temps et coût pour les traductions. – mauvaise qualité de certaines traductions, ce qui entraîne des retards dans le traitement des demandes.

3.6.2 Fondement juridique

Pays	Fondement juridique (Q 2.1.2)
Albanie	– Convention sur la cybercriminalité ; – Convention européenne sur l'entraide en matière pénale (CdE) – Loi albanaise sur les relations juridictionnelles avec des autorités étrangères en matière pénale
Arménie	Régi par l'article 499' 6 CPP de l'Arménie.
Australie	*Mutual Assistance en Criminal Matters Act 1987*, notamment section 15B ; *Telecommunications (Interception et Access) Act 1979,* sections 110, 116 et 117.
Autriche	– Accords internationaux, lorsqu'ils s'appliquent ; – Loi fédérale autrichienne sur l'Extradition et l'entraide judiciaire, notamment section 56 § 2 ;
Belgique	Loi du 9 décembre 2009.
Bosnie-Herzégovine	– Convention sur la cybercriminalité ; – Convention européenne sur l'entraide en matière pénale (CdE). Loi sur l'entraide en matière pénale (JO Bosnie-Herzégovine, no. 53/09, 58/13), articles 1-8. Code de procédure pénale de la Fédération de Bosnie-Herzégovine ; Code de procédure pénale de la Republika Srpska ; Code de procédure pénale du district de Brcko
Bulgarie	*Code de procédure pénale*, notamment article 471
Costa Rica	*Loi cadre du ministère public ; Code de procédure pénale*
Croatie	– Convention sur la cybercriminalité ; – Convention européenne sur l'entraide en matière pénale (CdE). Loi sur l'entraide internationale en matière pénale (JO 178/04)
Chypre	Loi de ratification de la Convention sur la cybercriminalité, 2004, et loi nationale sur la coopération internationale en matière pénale.
République dominicaine	*Accords bilatéraux et internationaux.*
Estonie	*Code de procédure pénale*, articles 462-463.
Finlande	– Loi sur l'entraide en matière pénale (4/1994) – Accords internationaux, lorsqu'ils s'appliquent.

Pays	Fondement juridique (Q 2.1.2)
France	*Code de procédure pénale*, articles 695-9-31 à 695-9-47 et articles R49-35 à R49-39.
Géorgie	*Loi sur la coopération internationale en matière pénale,* article 2.
Allemagne	*Section 59 de la Loi sur l'entraide en matière pénale*, conjointement à des accords internationaux et/ou au *Code de procédure pénale*, sections 94-100.
Hongrie	Loi sur l'entraide internationale en matière pénale, 1996. Act XXXVIII. Act 61-75. § Autres accords.
Islande	
Italie	n/a.
Japon	*Loi sur l'entraide internationale en matière d'enquêtes et autres affaires connexes*, plus particulièrement article 8
Lettonie	*Loi sur la procédure pénale*, article 845
Lituanie	*Loi no. IX-1974, 22 janvier 2004 sur la Ratification de la Convention sur la cybercriminalité* (JO 36-1178, 2004) ; *Code de procédure pénale*.
Moldova	*Code de procédure pénale de la République de Moldova*, article 536.
Monténégro	– Convention sur la cybercriminalité ; – Convention européenne sur l'entraide en matière pénale (CdE). Loi sur l'entraide judiciaire en matière pénale (JO du Monténégro, n° 04/08, 17 janvier 2008)
Pays-Bas	– Code de procédure pénale, titre X ; – Accords internationaux, le cas échéant.
Norvège	*Loi sur la procédure pénale* article 215a ; Loi sur les tribunaux, article 46
Philippines	Le fondement juridique pour l'exécution de demandes d'entraide est principalement l'Accord bilatéral entre les Philippines et un pays donné sur l'entraide judiciaire en matière pénale. Le fondement juridique sera différent en fonction des pays. Actuellement, les Philippines ont ce type d'accord avec les pays suivants : Royaume-Uni, Australie, États-Unis, Hong-Kong, Suisse, République de Corée, Inde, Espagne.
Portugal	*Loi sur la cybercriminalité*, articles 24 et 15
Roumanie	– Loi no. 302/2004 sur la coopération judiciaire internationale en matière pénale (republiée) ; – Loi no. 161/2003 Titre III (Prévention et lutte contre la cybercriminalité) ; – Loi no. 508/ 2004 sur la création, l'organisation et le fonctionnement de la Direction pour l'investigation en matière de crime organisé et de terrorisme ; – Loi 39/2003 sur la prévention et la lutte contre le crime organisé ; – Loi 656/2002 sur la prévention et la sanction du blanchiment d'argent

Pays	Fondement juridique (Q 2.1.2)
Serbie	– Convention sur la cybercriminalité ; – Convention européenne sur l'entraide en matière pénale (CdE). Loi serbe sur l'entraide judiciaire en matière pénale
Slovaquie	Fondement juridique : les dispositions des articles 537, 538, 539 du Code de procédure pénale sont combinées aux articles 90, 115,166 du Code de procédure pénale, en tant que de besoin.
Slovénie	*Code de procédure pénale*, notamment articles 148, 149b, 164, 220 et 515
Espagne	– *Loi 25/2007* (transposant la Directive 2006/24CE) et autres (loi sur juges, loi sur procureurs et *Code de procédure pénale*) ; – Accords internationaux applicables.
Suisse	*Loi fédérale sur l'entraide internationale en matière pénale* (Mutual Assistance Act, IMAC) du 20 mars 1981.
«l'ex-République yougoslave de Macédoine»	– Convention des Nations-Unies contre le crime organisé transnational – Convention sur la cybercriminalité. Code de procédure pénale, chapitre XXX.
Turquie	– Accords bilatéraux ; – Conventions multilatérales des Nations Unies ; – conventions de l'OCDE ; – Convention européenne sur l'entraide en matière pénale (CdE). – législation non spécifique sur l'entraide (en préparation). – existence d'une circulaire du MJ pour l'exécution des demandes d'entraide.
Ukraine	(MdI) *Code de procédure pénale*, articles 554-572. (Serv Sec) *Code de procédure pénale*, part IX (article 543).
Royaume-Uni	– The Crime (International Co-operation) Act 2003 (CICA) ; – Accords internationaux applicables.
États-Unis d'Amérique	Titre 18, *U.S.C.*, Section 3512.

3.6.3 Procédures (Question 2.4) et problèmes rencontrés (Question 2.5)

2.4 Procédure : procédure pas à pas pour envoyer/recevoir une demande et suites données aux demandes

En tant qu'Etat requis : veuillez décrire pas à pas la procédure complète que vous devez suivre lorsque vous recevez une demande concernant des données informatiques stockées.

En tant qu'Etat requérant : veuillez décrire pas à pas la procédure complète que vous devez suivre lorsque vous envoyez une demande concernant des données informatiques stockées.

2.5 Principaux problèmes en matière d'entraide concernant l'accès aux données stockées

Quels sont les principaux problèmes auxquels vous êtes confronté en tant qu'Etat requérant ? Veuillez donner des détails et des exemples.

Quels sont les principaux problèmes auxquels vous êtes confronté en tant qu'Etat requis ? Veuillez donner des détails et des exemples.

Pays	**Procédure pour l'envoi/la réception de demandes (Q 2.4)**	**Problèmes rencontrés (Q 2.5)**
Albanie	En tant qu'Etat *requérant* : – Demande pour l'obtention de données auprès de leur détenteur (FSI ou autre personne morale) avec l'assistance des services de poursuite (SP). Le point de contact étranger des SP est immédiatement contacté. – Entre-temps, une commission rogatoire formelle est envoyée aux autorités étrangères. En tant qu'*Etat requis* : – A réception, la demande est transmise par le ministère de la Justice au tribunal compétent ; – Le Tribunal décide de transmettre la demande au parquet ; – le parquet exécute la demande par le biais des services répressifs, FSI ou autres entités privées ;	En tant qu'Etat *requérant* : – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves). – Différence entre les systèmes judiciaires. En tant qu'Etat *requis* : – Restrictions légales fondées sur la protection des données à caractère personnel ; – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves). – Différence entre les systèmes judiciaires.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	– les données obtenues sont transmises à l'autorité judiciaire étrangère.	
Arménie	Le Bureau du Procureur général est responsable de la réception des demandes d'entraide.	En tant qu'Etat requérant : des pays étrangers refusent la coopération sans demande d'entraide. Celles-ci ne peuvent s'appliquer que pour une affaire pénale. Toutefois, or, les affaires pénales peuvent être entamées sans information épreuve suffisante au préalable. En tant qu'Etat requis : une injonction judiciaire est requise en Arménie pour obtenir les données. Cela peut prendre du temps était parfois refusé.
Australie	En tant *qu'Etat requéran*t : 1° il est possible, par le biais d'une demande informelle du pays étranger, de déterminer s'il est possible d'obtenir des données informatiques stockées et quels sont les seuils juridiques à respecter. L'Australie détermine s'il est possible de conserver ces données en attendant une demande officielle d'entraide judiciaire. 2° les services répressifs australiens cherchent à conserver les données informatiques stockées ; 3° le service de l'Attorney-General entre en contact avec les services répressifs ou les services de poursuite qui demandent les données informatiques stockées afin de veiller à ce qu'il y ait suffisamment d'informations indiquées dans une demande formelle aux pays étrangers pour que les seuils légaux étrangers soient respectés ; 4° le service de l'Attorney General envoie une demande formelle d'entraide judiciaire au pays étranger demandant les données informatiques stockées ; 5° il assure la liaison avec le pays étranger concernant la remise	En tant *qu'Etat requérant* : – veiller à ce que la demande respecte les seuils juridiques du pays étranger pour fournir des données stockées (solution possible : contact direct, si cela est possible, avec les autorités centrales étrangères pour conseils sur la manière de respecter les seuils) ; – veiller à ce que le matériel soit préservé et ne soit pas effacé avant que la demande officielle ne soit faite et que l'injonction ait été exécutée pour obtenir ces données ; – temps nécessaire pour obtenir des données stockées de la part de pays étrangers (souvent au minimum de 6 à 12 mois). En tant *qu'Etat requis* : – manque d'informations suffisantes dans la demande, ce qui entraîne une perte de temps et de ressources pour demander des informations supplémentaires. Cela peut également empêcher les autorités australiennes de vérifier que les seuils sont respectés, et il est possible dans ce cas que l'on n'obtienne pas l'autorisation pour l'injonction.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	des données informatiques stockées. En tant *qu'Etat requis* : 1° demande d'un pays étranger 2° autorisation de l'Attorney-General ; 3° demande de l'officier de police australien à l'autorité judiciaire compétente pour obtenir une injonction concernant les données informatiques stockées ; 4° l'autorité judiciaire examine la demande d'injonction et peut lui donner suite ; 5° accès aux communications stockées ; 6° transmission du matériel au pays étranger.	
Autriche	En tant *qu'Etat requérant* : 1° Préparation de la demande par le Procureur compétent (avec traduction et « légalisation » des documents) ; 2° Transmission de la demande soit directement, soit par le biais de l'autorité centrale (par les canaux diplomatiques en l'absence d'accord international). En tant *qu'Etat requis* : 1° Réception de la demande soit directement par l'autorité d'exécution, soit par le ministère fédéral de la Justice (en fonction des accords internationaux) ; 2° Après vérifications légales, transmission de la demande par le MJ au service de poursuite compétent localement pour exécution de celle-ci ; 3° Le cas échéant, délivrance d'une injonction par le procureur avec l'accord du tribunal ; 4° Exécution de l'injonction par la police sous la supervision du service de poursuite. 5° Transmission des résultats à l'Etat requérant soit directement	En tant *qu'Etat requérant* : – Refus de demandes concernant des infractions vénielles ; – Manque de connaissances des délais légaux en matière de stockage de données. En tant *qu'Etat requis* : – manque de la documentation requise par le droit national (voir Q 2.1.1) – manque de clarté de la demande (type of données ; période concernée pour la production des données).

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	soit par l'autorité centrale.	
Azerbaïdjan	En qu'Etat requérant : L'autorité centrale reçoit une demande ; L'autorité centrale obtient les données de la part des fournisseurs de services (et etc.) suite à une décision de justice Suites aux procédures internes, l'autorité centrale envoie les données à l'Etat requérant.	
Belgique	En tant *qu'Etat requérant* : Voir ci-dessous modus modendi. En tant qu'Etat requis : la demande est reçue directement par l'autorité judiciaire étrangère. Si elle est envoyée à l'autorité centrale (en Belgique, le Service fédéral de poursuites), celle-ci la transmet à l'autorité judiciaire territoriale compétente. Si elle concerne plusieurs autorités ou si l'on ne voit pas clairement laquelle est responsable, c'est le Service fédéral de poursuites qui l'exécute ou en coordonne l'exécution. Un juge d'instruction n'intervient que si des mesures coercitives sont requises, par exemple pour l'obtention de données informatiques stockées.	Retard dans le temps pris à répondre. L'obtention de données dépend des politiques internes des entreprises. Certaines d'entre elles exigent une demande d'entraide judiciaire, d'autres sont en mesure de donner directement des données relatives au trafic à un service de poursuites. L'obtention de données relatives au contenu exige un certain niveau de preuve qu'il n'est pas possible d'atteindre à moins d'obtenir effectivement les données (cercle vicieux).
Bosnie-Herzégovine	En tant *qu'Etat requérant* : – transmission de la demande par le ministère de la Justice ; (exception, prévue dans les traités : transmission directe par les autorités judiciaires nationales à leurs homologues étrangers ; utilisation des canaux d'Interpol, utilisation d'Eurojust) En tant *qu'Etat requis* : – transmission de la demande, par le biais du ministère de la Justice, à l'autorité judiciaire compétente (exception :	En tant *qu'Etat requérant* : – on ne sait pas à qui s'adresser en cas d'urgence (par exemple pour sécuriser des données jusqu'à ce qu'une demande officielle d'entraide judiciaire soit transmise). En tant *qu'Etat requis* : n/a.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	transmission directe par Interpol en cas d'urgence). En l'absence de traité, ou lorsque ceci est envisagé par un traité, le ministère de la Justice transmet ou reçoit des demandes par le biais du ministère des Affaires étrangères. – La police informe le procureur de tous les faits pertinents, et demande son accord. – À la suite de cet accord, le tribunal compétent délivre une injonction à l'opérateur de télécommunications (pour la fourniture de données par un fournisseur de services sur Internet). La police applique ensuite l'injonction judiciaire.	
Bulgarie	En tant qu'Etat requérant : la demande doit être transmise au ministère de la Justice (excepté en cas de procédure différente prévue dans un accord international). En tant qu'Etat requis : n/a. [à clarifier]	En tant qu'Etat requérant : des retards ou inexécution des demandes par les autorités dans certains pays. En tant qu'Etat requis : pas de problèmes spécifiques.
Costa Rica	En tant *qu'Etat requérant* : 1° coordination de la préparation de la demande par le procureur compétent et le Bureau des conseils techniques et relations internationales (OATRI) (forme de preuves requise ; type d'infraction ; faits ; niveau d'urgence etc.) ; 2° identification par l'OATRI de l'instrument de coopération applicable et de l'autorité centrale compétente pour le traité ; 3° (a) si l'autorité centrale est l'OATRI, la demande est directement envoyée à l'autorité centrale compétente dans l'État requis ; 3° (b) si l'autorité centrale est une autre institution, la demande est transmise à cette dernière, qui la transmet à son tour à l'autorité centrale de l'État requis ;	En tant qu'Etat requérant : dans une affaire particulière, une demande de données concernant le compte utilisateur d'un réseau social aux États-Unis a été refusée au motif qu'elle n'atteignait pas un seuil de priorité En tant qu'Etat requis : n/a.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	4° une fois la demande exécutée et une réponse reçue, l'OATRI vérifie qu'elle a suivi les canaux applicables et transmet la réponse au procureur compétent. En tant *qu'Etat requis* : 1° l'OATRI reçoit la demande (directement lorsqu'il s'agit d'une autorité centrale, ou indirectement par le biais de l'autorité centrale compétente) ; 2° analyse par l'OATRI du respect par la demande des conditions requises par les instruments applicables en droit national, et traitement d'autres problèmes (par exemple les questions pour les témoins) ; 3° identification par l'OATRI de l'autorité compétente pour l'exécution de la demande (procureur, l'OATRI lui-même etc.) ; 4° vérification par l'OATRI que l'exécution est conforme à ce qui était demandé et au droit national, et envoi des demandes par le biais de l'autorité centrale ou d'autres canaux appropriés (canal diplomatique par exemple).	
Croatie	En tant *qu'Etat requérant* : – le tribunal compétent transmet une demande officielle (au ministère de la Justice) – le ministère de la Justice envoie une demande officielle à l'État requis ; – à réception d'une réponse, le ministère de la Justice la transmet au tribunal qui a entamé le processus de demande. En tant qu'Etat requis : – À réception par le ministère de la Justice, transmission de la demande au tribunal compétent ; – – une fois que le tribunal a exécuté la demande, une réponse est envoyée à l'État requérant.	En tant *qu'Etat requérant* : Temps pris avant de recevoir une réponse à la demande. En tant *qu'Etat requis* : n/a.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
Chypre	En tant qu'Etat requis : 1. Dès qu'une demande est reçue, la police demandera à un tribunal une injonction pour obtenir les données stockées. 2. Demande aux fournisseurs de services sur Internet pour obtenir les informations sur le propriétaire de l'ordinateur 3. Demande à un tribunal pour une injonction de perquisition domiciliaire ou de l'ordinateur du suspect. En tant qu'Etat requérant : À la suite d'une enquête, une demande d'entraide judiciaire est envoyée via le ministère de la Justice et de l'Ordre public.	En tant qu'Etat requis : Surcharge de demandes. En tant qu'Etat requérant : Beaucoup de temps pour préparer tous les documents pertinents et la procédure afin d'envoyer la demande d'entraide judiciaire, et beaucoup de temps pour recevoir une réponse à la demande.
République dominicaine		Les informations demandées ne sont en général pas reçues à temps.
Estonie	En tant *qu'Etat requérant* : ["Voir ci-dessus". [à clarifier]]. En tant *qu'Etat requis* : 1. après vérification des conditions légales et juridiques par le ministère de la Justice, transmission de la demande au Bureau du procureur public ; 2. après vérification par ce dernier de l'admissibilité et de la faisabilité des mesures demandées dans la demande, transmission à l'autorité judiciaire compétente pour exécution ; 3. envoi des matériels obtenus au ministère de la Justice via le Bureau du procureur ; 4. transmission du matériel par le ministère de la Justice à l'État requérant (ou via EUROJUST, pour les demandes envoyées par ce biais) (*) en cas d'urgence : les demandes soumises via les canaux d'Interpol ou d'une notice Schengen peuvent être exécutées avec l'accord du Bureau du procureur, avant qu'une demande officielle d'entraide judiciaire ne soit reçue par le ministère de la Justice	En tant *qu'Etat requérant* : – non-conservation des données dans les États requis, même certaines Parties à la Convention sur la cybercriminalité ; – Difficulté de coopération avec des États non membres de l'UE (absence de réponse). En tant *qu'Etat requis* : pas de problème, surtout depuis que les demandes concernant des adresses IP ne sont plus considérées comme une activité de surveillance.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
Finlande	*En tant qu'Etat requérant* : 1. préparation de la demande par le Bureau national d'investigation ou par un service de police locale ; 2. transmission de la demande au Bureau national d'investigation pour contrôle qualité et traduction dans la langue étrangère ; 3. envoi de la demande (a) (pays non membres de l'Union européenne) par le ministère de la Justice, ou (b) (pays membres de l'Union européenne) directement par le Bureau national d'investigation à l'État requis. Dans l'UE, pour des affaires de mandat européen d'obtention de preuves, un procureur émet dans la plupart des cas ce type de demande. En général, le procureur a un rôle essentiel à jouer pour évaluer si une demande d'entraide judiciaire doit être émise et pour quels problèmes. Les autorités de police et de poursuite ont l'obligation de coopérer dans des enquêtes criminelles. En tant *qu'Etat requis* : 1. réception de la demande par (a) (pays non membres de l'UE), le ministère de la Justice, ou directement les autorités compétentes ; la demande est ensuite transmise au Bureau national d'investigation ; ou (b) (pays membres de l'UE) directement au Bureau national d'investigation. 2. vérification des conditions légales par ce dernier ; 3. exécution de la demande par ce dernier ou par un service de police local, y compris par le biais de mesures coercitives si cela est légalement possible 4. compilations des preuves par le Bureau national d'investigation ; 5. envoi de documents (a) (pays non membres de l'UE) au ministère de la Justice, qui les transmettra ensuite à l'État	En tant *qu'Etat requérant* : – temps nécessaire lorsque la demande est envoyée via le canal des ministères de la Justice ; – temps nécessaire pour obtenir des réponses de la part de certains pays. En tant *qu'Etat requis* : – demandes reposant sur une base faible, ce qui indique un manque de contrôle de la qualité dans l'Etat requérant. – non-respect de tous les critères légaux applicables.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	requérant ; ou (b) (pays membres de l'UE) directement à l'État requérant.	
France	[à clarifier] 1 En tant *qu'Etat requérant* : depuis 2012, toute demande transmise via les canaux d'Interpol passe par l'Unité nationale, qui la transmet au Bureau national étranger requis. En tant qu'Etat requis : 1° la demande reçue par le biais des canaux d'Interpol est enregistrée dans une base de données internationale contenant tous les emails au sein de la Direction ; 2° la demande est traitée par la section de documentation opérationnelle	En tant *qu'Etat requérant* : Difficulté à obtenir des données personnelles sans commission rogatoire. En tant *qu'Etat requis* : – impossibilité pour la police nationale de transmettre des données personnelles exigeant l'émission d'une injonction judiciaire – même pour de simples demandes d'adresse IP ; – charge de travail entraînée par les commissions rogatoires pour des informations de base comme celles-là ; – demandes concernant une affaire isolée ou un préjudice limité (par exemple demandes d'informations concernant une fraude à la carte de crédit pour laquelle le préjudice était de 750 €).
Géorgie	En tant *qu'Etat requérant* : 1. transmission de la demande par les services répressifs pertinents au ministère de la Justice ; 2. vérification des conditions légales par le ministère de la Justice ; 3. envoi de la demande par (a) (étape du procès) du ministère de la Justice lui-même, ou (b) (durant le recueil de renseignements criminels) par sa sous-division, le Bureau du procureur général. En parallèle, les informations sont fournies à l'État requis en ce qui concerne les délais préférés pour exécuter la requête la demande. En tant *qu'Etat requis* :	En tant *qu'Etat requérant* : procédure d'entraide retardée (par exemple pour identifier l'autorité compétente qui pourra fournir les informations nécessaires). En tant *qu'Etat requis* : obstacles techniques rencontrés (ainsi, difficultés pour les fournisseurs de services sur Internet nationaux à stocker les journaux d'accès et de serveurs pendant une durée suffisante). n/a. Pas d'expérience.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	1. traduction de la demande ; 2. vérification par les services de poursuite des conditions formelles et des motifs potentiels de refus 3. transmission de la demande à l'organe interne le plus pertinent pour suite à donner, et communication des informations à l'État requérant en ce qui concerne le temps nécessaire pour l'exécution ; 4. envoi de la réponse, avec informations et documentation, à l'État requérant via les canaux diplomatiques ou autres canaux directs.	
Allemagne	En tant *qu'Etat requérant* : 1. examen pour savoir si les données ont été provisoirement conservées et, si tel n'est pas le cas, recommandations en ce sens ; 2. vérification du respect des conditions légales de l'État requis pour ce qui est de la demande ; 3. envoi de la demande, avec sa traduction, à l'État requis. En tant *qu'Etat requis :* 1. contact préliminaire par le point de contact 24/7 avec le procureur compétent sur le possible déclenchement d'une enquête au niveau national ; 2. les données peuvent avoir déjà été sécurisées sur émission d'une injonction par (a) un tribunal ; ou (b) la police ou le procureur (dans des conditions exceptionnelles et si cela ne concerne pas des données de trafic) ; 3. réception officielle de la demande d'entraide judiciaire ; 4. vérification des conditions légales par le Bureau fédéral	En tant *qu'Etat requérant :* – fortes exigences imposées pour la déclaration des faits, ce qui exige le recueil d'informations supplémentaires et retarde l'exécution de la demande ; – temps nécessaire pour l'exécution des demandes concernant des données liées aux abonnés En tant *qu'Etat requis :* aucun problème signalé jusqu'ici.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	de la justice, et vérification que les données ont été conservées à titre provisoire ; 5. transmission de la demande à l'autorité judiciaire compétente du Land ; 6. transmission des données saisies à l'État requérant.	
Hongrie	En tant *qu'Etat requis* : Réception de la demande => Traduction => envoi de la demande à l'opérateur compétent => Réception de la réponse => Traduction => Envoi de la réponse au pays requérant En tant *qu'Etat requérant* : L'autorité d'investigation hongroise envoie la demande au Centre hongrois pour la coopération internationale => Traduction => Envoi de la demande au centre de coopération internationale judiciaire du pays concerné => Réception de la réponse => Traduction => Envoi de la réponse à l'autorité requérante.	En tant *qu'Etat requérant* : Une commission rogatoire est nécessaire pour obtenir la liste d'appels. En tant *qu'Etat requis :* Essentiellement, une commission rogatoire est nécessaire pour obtenir la liste d'appels.
Islande	En tant qu'Etat requérant : Le Ministère reçoit une demande d'entreaide soit depuis district les commissaires de Police de District ou du Bureau spécial du procureur. Le ministère garantit que la demande est faite suffisamment et envoie formellement la demande à l'autorité compétente de l'État requis.	En tant qu'État requis : Toutes les demandes sont transmises au ministère de l'intérieur à moins que d'autres arrangements aient été décidés par un accord avec un autre État. Le ministère étudie la demande et la rejette si les conditions légales ne sont pas réunies, ou s'il est clair que la demande ne peut être accordée. Si une demande n'est pas rejetée, le ministère envoie l'affaire au directeur des poursuites publiques pour un traitement ultérieur. Le DPP ordonne l'enquête nécessaire à effectuer, habituellement par le commissaire de Police de District compétent ou le Bureau du procureur spécial. Lorsque l'enquête a été menée le DPP envoie la preuve recueillie au ministère, accompagnée d'un rapport à ce sujet, et le ministère les transmet à l'autorité compétente dans l'État

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
		requérant.
Italie	En tant *qu'Etat requérant* : 1. identification des informations nécessaires ; 2. présentation de la demande au personnel d'encadrement pour approbation ; 3. après approbation, envoi de la demande auprès de contact pertinent. En tant *qu'Etat req*uis : La demande est reçue, examinée, évaluée et transmise à l'unité ou division compétente.	En tant *qu'Etat requérant* : Absence de réponses aux demandes d'entraide dans certains cas. En tant *qu'Etat requis* : Réception tardive des demandes, ce qui empêche les autorités de conserver les données dans les délais.
Japon	En tant qu'Etat *requérant* : 1ère situation : demande basée sur un accord d'entraide judiciaire ; envoi de la demande à l'autorité centrale étrangère par (a) la Commission nationale pour la sécurité publique (NPSC) pour des demandes émanant d'une police préfectorale, ou (b) par le ministère de la Justice pour des demandes émises par le Bureau du procureur ; 2e situation : demande ne reposant pas sur un accord d'entraide judiciaire ; envoi de la demande à l'autorité centrale étrangère par le ministère des Affaires étrangères, sur demande de l'Agence nationale de la police ou du ministère de la Justice. En tant *qu'Etat requis* : 1ère situation : demande reposant sur un accord d'entraide judiciaire 1. réception de la demande par le ministère de la Justice ; 2. injonction du ministère de la Justice à l'autorité compétente ((procureur principal, Commission) de recueillir les preuves ;	En tant qu'Etat r*equérant* : Temps nécessaire pour recevoir les informations demandées. Exemple : affaire impliquant le téléchargement illégal de produits protégés par le droit de la propriété sur des sites étrangers. L'obtention des informations (y compris les données des journaux de téléchargement) a pris 112 jours, soit plus que le délai fixé pour la conservation des données par le FSI gérant les adresses IP impliquées. >Il n'a donc pas été possible de pister les renseignements concernant des abonnés connectés à ces adresses. En tant *qu'Etat requis* : manque d'informations suffisantes dans la demande pour justifier l'émission d'une injonction du tribunal nécessaire pour la perquisition et la saisie de données.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	3. transmission des preuves recueillies par l'autorité compétente au ministère de la Justice ; 4. transmission des preuves par le ministère de la Justice à l'État requérant ; <u>2e situation</u> : demande ne reposant pas sur un accord d'entraide judiciaire 1. réception de la demande par le ministère des Affaires étrangères par le biais des canaux diplomatiques, qui le transmet au ministère de la Justice ; 2. injonction par le ministère de la Justice à l'autorité compétente (voir ci-dessus) de recueillir les preuves ; 3. envoi des preuves recueillies par l'autorité compétente au ministère de la Justice ; 4. transmission des preuves au ministère des Affaires étrangères, qui les transmet ensuite à l'autorité diplomatique de l'État requérant	
Lettonie	En tant *qu'Etat requérant* : 1° la personne en charge des procédures au niveau national transmet une proposition écrite (définissant la forme et le contenu de la demande) aux autorités compétentes pour demander une action procédurale par l'État requis ; 2° préparation de la demande, contenant les documents exigés au titre du droit national (notamment une injonction du tribunal) et respectant la procédure applicable ; 3° si la demande est jugée justifiée, elle est alors traduite et envoyée à l'État requis. En tant *qu'Etat requis :* 1° Réception de la demande pour la divulgation de données stockées ;	En tant *qu'Etat requérant* : temps nécessaire pour avoir des réponses (jusqu'à 2 ans). [à clarifier] En tant *qu'Etat requis* : les problèmes ne sont pas identifiés

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	2° Décision de l'autorité compétente sur l'admissibilité de l'action procédurale demandée ; 3° Exécution de la demande conformément au droit national sur la procédure pénale (note : les preuves matérielles nécessaires, telles que les dispositifs contenant des données stockées, peuvent être transmises).	
Lituanie	En tant *qu'Etat requérant* : 1° Préparation de la demande par le point de contact national ; 2° (i) Envoi de la demande par le réseau 24/7 ; (ii) préparation, en parallèle, de la demande d'entraide, qui est ensuite envoyée au Bureau du procureur général pour suites à donner. En tant *qu'Etat requis* : 1° réception d'une demande pour des données informatiques stockées, le point de contact national demande immédiatement la conservation des données requises par le FSI concerné ; 2° A réception de la demande d'entraide, toutes les actions demandées possibles sont réalisées.	En tant *qu'Etat requérant* : – manque d'informations actualisées sur la législation ; – conditions formelles exigées par certains États étrangers. En tant *qu'Etat requis* : Pas de problèmes fondamentaux.
Moldova	(Sur la base d'accords internationaux ou de la réciprocité) En tant qu'Etat requérant : (a) Transmission de la demande, par l'organe de poursuite pénale au procureur général, pour que celle-ci soit envoyée pour exécution dans l'État requis ; (b) Transmission de la demande par le tribunal compétent au ministère de la Justice, qui la fait suivre pour exécution à l'Etat requis. En tant *qu'Etat requis* : – à réception de la demande de celle-ci est transmise par (a) le bureau du procureur général aux échanges et de l'enquête criminelle ou, le cas échéant, par le ministère de la Justice au	En tant *qu'Etat requérant* : – problèmes de temps (durée de la procédure ; problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves). – Différence entre les systèmes judiciaires. En tant *qu'Etat requis* : – restrictions légales fondées sur la protection des données à caractère personnel ; – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves). – différences entre les systèmes judiciaires. Nécessité d'améliorer les techniques spéciales, les capacités institutionnelles du personnel pour la coopération et de partager les bonnes pratiques et les

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	tribunal compétent – des accords internationaux ou accords de réciprocité peuvent prévoir des procédures spécifiques au titre du droit de l'Etat requérant, où l'assistance des autorités requérantes pour l'exécution de la demande – lorsque l'exécution de la demande n'est pas possible, les documents sont renvoyés à l'État requérant avec les informations justifiant le refus.	expériences en matière de cybercriminalité.
Monténégro	En tant *qu'Etat requérant* : (en l'absence d'accord international) – l'autorité qui souhaite obtenir les données prépare une commission rogatoire et la transmet au ministère de la Justice – après vérification légale, celui-ci envoie la demande à l'Etat requis. En tant *qu'Etat requis* : – à réception par le ministère de la Justice, transmission de la demande à l'autorité judiciaire compétente ; – l'autorité judiciaire compétente exécute la demande et collecte les données recherchées.	En tant *qu'Etat requérant* : Manque d'expérience. En tant *qu'Etat requis* : Manque d'expérience.
Pays-Bas	En tant *qu'Etat requérant* : 1° Enregistrement de la demande, et envoi au Bureau national pour l'entraide internationale en matière pénale ; 2° Envoi formel de la demande par le Bureau, soit (a) (pays membres de l'UE) directement, ou (b) (pays non-membres de l'UE) via l'autorité centrale au ministère de la Sécurité et de la Justice. En tant *qu'Etat requis* : 1° Réception de la demande par le biais du réseau 24/7, du ministère de la Sécurité et de la Justice ou du Bureau national des procureurs (National Procureurs' Office - NPO) ;	En tant *qu'Etat requérant* : – Temps nécessaire pour traduire les demandes. – on ne sait pas quelle autorité intervient sur la demande dans l'Etat requis. En tant *qu'Etat requis* : – caractère très large de la demande, ce qui complique énormément son exécution ; – recherche insuffisante (par exemple l'Etat requis n'est pas le bon pour les données recherchées).

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	2° Examen de la demande par le NPO, et décision avec l'équipe criminalité high-tech de la Police nationale pour savoir qui devrait exécuter la demande : (a) des unités régionales de la Police nationale, ou (b) l'équipe criminalité high-tech ; 3° Exécution : (a) (unités régionales de la police) transmission de la demande à une antenne locale pour l'entraide international en matière pénale ; (b) (équipe criminalité high-tech) transmission de la demande à l'équipe, qui l'enregistre et lui donne un nom ; contrôle de capacité et réalisation des actions nécessaires pour obtenir des permissions applicables auprès des autorités judiciaires ; envoi des résultats de l'exécution au NPO. 4° Envoi des résultats soit directement à l'Etat requérant, soit via un juge.	
Norvège	En tant *qu'Etat requérant* : 1° identification de l'Etat à qui la demande devrait être adressée ; 2° (a) (urgence) envoi direct de la demande, suivi d'une demande formelle ; (b) (affaires normales) demande par le Procureur au tribunal national pour une décision judiciaire déclarant que les conditions légales nationales pour l'accès aux données sont remplies – à envoyer avec la demande. En tant *qu'Etat requis* : 1° traitement de la demande par le Procureur (typiquement NCIS Norvège/Kripos) ; 2° identification de la cible, clarification de la situation de la personne/entreprise en tant que suspect ou tiers ; 3° délivrance d'une injonction de tribunal pour la perquisition ou production de données (en urgence : directement par le Procureur, avec examen ultérieur par le Tribunal). Certains types de données (par exemple des informations sur un client auprès	En tant *qu'Etat requérant* : – temps nécessaire pour traiter les demandes (environ un an pour obtenir des données relatives au contenu dans une affaire de meurtre spécifique liée au crime organisé) ; – différences entre les systèmes judiciaires ; – identification difficile de l'autorité ciblée pour la demande (en particulier pour les services d'hébergement sur le web). En tant *qu'Etat requis* : Réception tardive de certaines demandes, en particulier concernant des journaux d'IP, effacés par les FSI après 21 jours. Suggestion : l'Etat requérant devrait entrer en contact très rapidement pour s'assurer que les données sont préservées (via la conservation accélérée ou par une enquête parallèle).

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	d'un FSI) peuvent être directement demandées à la société ; 4° une fois les preuves obtenues et/ou analysées, le Procureur et/ou l'enquêteur contactent souvent l'Etat requérant pour déterminer comment les preuves devraient être transmises ; 5° si le ministère de la Justice a reçu la demande initiale, les documents devraient être transmis par le même canal.	
Philippines	La procédure dépendrait de l'accord bilatéral particulier régissant l'entraide pénale entre les Philippines et le pays concerné.	En tant qu'Etat requérant : complexité du système En tant qu'Etat requis : absence d'une loi.
Portugal	En tant qu'Etat *requérant* : 1° transmission de la demande au Bureau du Procureur général (autorité central pour les demandes de coopération) ; 2° envoi de la demande à l'autorité centrale de l'Etat requis ; 3° réception de la réponse par le canal des autorités centrales. En tant qu'Etat *requis* : 1° réception de la demande par le Bureau du Procureur général ; 2° transmission de la demande au ministère de la Justice pour qu'il tranche sur son admissibilité ; 3° envoi de la demande à l'autorité judiciaire compétente, qui exécute la demande – avec la coopération de la police si nécessaire ; 4° après l'exécution, transmission de la réponse par l'autorité judiciaire à l'autorité centrale, qui l'envoie à l'autorité centrale de l'Etat requérant. note : l'Accord Schengen permet le contact direct entre autorités judiciaires, raccourcissant la procédure entre ses Parties.	En tant qu'Etat *requérant :* – manque d'autonomie pour demander des données relatives au trafic ; – absence des données recherchées dans l'Etat requis. En tant qu'Etat *requis* : – pouvoirs limités de la police judiciaire, qui ne peut que demander la conservation des données.
Roumanie	En tant *qu'Etat requérant* : 1° Préparation de la demande par le Procureur qui mène l'enquête et les poursuites pénales ;	En tant *qu'Etat requérant* : – beaucoup de temps pour l'exécution des demandes (3-6 mois dans certains États) ;

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	2° Soumission de la demande par le Bureau pour l'entraide internationale (Office of International Legal Assistance - OILA) au sein de la Direction chargée des enquêtes sur le crime organisé et le terrorisme (DIICOT), soit (a) directement à l'autorité judiciaire requise, soit (b) à l'autorité centrale (ministère de la Justice). En tant *qu'Etat requis* : 1° réception de la demande par courrier, fax ou email ; 2° enregistrement de la demande par le DIICOT, et affectation à un Procureur de l'OILA ; 3° exécution par l'OILA, ou envoi pour exécution aux bureaux et services territoriaux du DIICOT. Pour certaines mesures, le Procureur devra demander l'accord du juge compètent (une procédure spécifique s'applique pour les demandes d'interception). En principe, le FSI ou autre détenteur de données devrait communiquer les données stockées dans les 48 heures. 4° envoi des données obtenues à l'autorité requérante.	– demandes rejetées pour des motifs d'absence de gravité/préjudice, ou pour des raisons budgétaires ; – pour des infractions interétatiques, les autorités judiciaires requises devraient estimer la complexité de l'enquête tout entière et non pas uniquement au regard du préjudice subi ; – différences entre les systèmes judiciaires, en particulier pour ce qui est des conditions liées à l'interception et à l'enregistrement de communications. En tant *qu'Etat requis* : – demandes pour des données dont le délai de conservation (6 mois) a expiré.
Serbie	En tant *qu'Etat requérant* : – Demande, par le parquet, pour l'obtention de données auprès des détenteurs (FSI ou autres personnes morales) grâce à une demande d'entraide. Le point de contact pour les DEJ est immédiatement contacté. – Lorsque les données ne peuvent être obtenues par ce moyen, une commission rogatoire formelle est envoyée aux autorités étrangères. En tant *qu'Etat requis* : – à réception de la demande, démarrage des mesures nécessaires ; – le parquet exécute la demande par la DEJ, auprès du FSI ou	En tant *qu'Etat requérant* : – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves) – Différence entre les systèmes judiciaires. En tant *qu'Etat requis* : – absence de l'infraction pénale dans le droit national ; – restrictions légales fondées sur la protection des données à caractère personnel ; – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves). – différences entre les systèmes judiciaires.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	autres entités privées ; – les données obtenues sont transmises à l'autorité judiciaire étrangère.	
Slovaquie	En tant qu'Etat requérant : Après réception des informations sur la conservation des données provenant du point de contact 24/7, un procureur rédige une demande d'entraide. Le projet est habituellement contrôlé par l'Autorité judiciaire centrale (le Bureau du Procureur général). Une traduction jurée est réalisée par un traducteur compétent. Enfin, la demande est transmise par les canaux et moyens disponibles (en fonction des conditions du traité applicable). En tant qu'Etat requis : Lorsqu'une demande est reçue, elle est envoyée au parquet (Bureau du Procureur général). Le contenu d'une demande (ainsi que la compétence de l'autorité requérante pour émettre une telle demande) est examiné par le Procureur, qui décide des mesures à prendre (une traduction jurée doit être assurée, si la demande n'est pas transmise en slovaque, des informations complémentaires peuvent être demandées, la police peut être autorisée à intervenir, un tribunal doit être saisi éventuellement).	En tant qu'Etat requérant : avant tout, il est important de recevoir les informations sur la conservation des données le plus tôt possible avec les références pertinentes à l'affaire dans l'Etat requis. En tant qu'Etat requis : Il est important que la demande d'entraide comporte une description suffisante de l'infraction, les noms des personnes impliquées, les lieux et dates de l'infraction, le préjudice causé, les liens avec la Slovaquie, et la lettre devrait être dûment signée et tamponnée, si cela peut se faire. Pour certaines actions, il faut des injonctions de justice et le critère de la double incrimination doit être rempli. C'est pourquoi il est très important que les informations sur l'affaire soient complètes pour satisfaire aux critères nationaux.
Slovénie	En tant *qu'Etat requérant* : 1° transmission de la demande par le service de police compètent au Secteur pour la coopération policière internationale (IPCS) ; 2° traduction de la demande, qui est ensuite envoyée à l'Etat requis. En tant *qu'Etat requis* : 1° réception de la demande par l'IPCS, qui la traduit en slovène ; 2° affectation de la demande au service de police compétent ;	En tant *qu'Etat requérant* : – temps nécessaire avant la réponse par l'Etat requis ; – absence de réponse par l'Etat requis. En tant *qu'Etat requis* : Dans certains cas, réticence des autorités judiciaires à appliquer les dispositions de la Convention sur la cybercriminalité, qui privilégient la demande d'entraide.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	3°mise en œuvre de mesures conservatoires, si demandé et si possible ; 4° obtention des données avec une lettre officielle de la police ou une injonction du tribunal, puis envoi à l'Etat requérant.	
Espagne	En tant *qu'Etat requérant* : 1° transmission de la demande au ministère de la Justice ; 2° après vérifications légales, (a) (lorsque les conditions ne sont pas remplies) la demande est renvoyée à l'autorité requérante, pour être complétée ; (b) (lorsque les conditions sont remplies) la demande est transmise à l'autorité centrale de l'Etat requis. En tant *qu'Etat requis* : 1° réception de la demande par le ministère de la Justice ; 2° après vérifications légales par le MJ, transmission de la demande pour exécution à l'autorité judiciaire compétente.	En tant *qu'Etat requérant* : difficultés à transmettre les très nombreuses informations demandées par l'Etat requis, en particulier du fait que la plupart des demandes sont envoyées à un stade précoce ; En tant *qu'Etat requis :* Pas de problème spécifique.
Suisse	En tant *qu'Etat requérant* : 1° examen sommaire (traduction, etc.) ; 2° demande de mesures (uniquement les mesures que les autorités nationales pourraient elles-mêmes accorder). En tant *qu'Etat requis* : 1° examen sommaire (traduction, autorité requérante) ; 2° désignation de l'autorité de poursuite (Procureur fédéral ou cantonal) ; 3° émission de l'injonction initiale (conditions : respect du principe de double incrimination, proportionnalité et accord du tribunal si nécessaire) ; 4° obtention des données ; 5° émission de l'injonction finale ; 6° Ev. Recours légaux.	En tant *qu'Etat requérant* : – absence de confirmation de la réception de la demande ; – critères divergents pour qualifier une demande « d'urgente ». En tant *qu'Etat requis* : – présentation insuffisante des faits (modus operandi) ; – demande concernant des données stockées depuis plus de 6 mois (autrement dit, délai de conservation obligatoire des données par les FSI dépassé).
«l'ex-République	En tant *qu'Etat requérant* :	En tant *qu'Etat requérant* : n/a.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
yougoslave de Macédoine»	– la demande du tribunal compétent est transmise par les canaux diplomatiques (du ministère aux autorités étrangères) En tant *qu'Etat requis* : – la demande des autorités étrangères est présentée par le ministère des Affaires étrangères au ministère de la Justice ; – Le MJ la transmet au tribunal compétent pour exécution ; - en cas d'urgence, the ministère de l'Intérieur peut traiter directement des demandes (condition : réciprocité).	En tant *qu'Etat requis* : n/a.
Turquie	En tant *qu'Etat requérant* : – préparation de la demande par le Procureur, qui la transmet à l'autorité centrale ; – après vérifications légales, la demande est envoyée à l'autorité étrangère. En tant *qu'Etat requis* : – l'autorité centrale (Direction générale du droit international et des relations extérieures) reçoit la demande ; – elle la transmet à l'autorité compétente ; – le Procureur local exécute la demande, en émettant directement un mandat destiné au FSI (données sur l'abonné), ou via une injonction de tribunal (données relatives au trafic et données relatives au contenu) rendue par un juge. – une fois les données obtenues du FSI, elles sont envoyées à l'autorité centrale, qui les transmet à l'Etat requérant.	En tant *qu'Etat requérant* : – problèmes de temps (durée de la procédure ; délais serrés pour traiter les preuves) ; – différence entre les systèmes judiciaires ; – difficulté à coopérer avec certains FSI ; – problèmes dans le fonctionnement de la coopération au niveau des points de contact ; – traductions non satisfaisantes. En tant *qu'Etat requis* : n/a.
Ukraine	(MdI) En tant *qu'Etat requérant* : 1° accord du Procureur ; 2° envoi de la demande par une autorité compétente (juge, procureur ou enquêteur) à l'autorité (centrale) compétente pour	(MdI) En tant *qu'Etat requérant* : délais courts pour traiter la demande (un mois, avec possibilité de prorogation sur autorisation). En tant *qu'Etat requis* : pas de problèmes.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	l'entraide ; 3° après vérifications légales, envoi de la demande dans les 10 jours par l'autorité (centrale) compétente à l'autorité compétente de l'Etat requis, soit directement, soit par les canaux diplomatiques ; 4° En cas de refus, tous les documents sont renvoyés dans les 10 jours avec une explication du motif de refus. En tant *qu'Etat requis* (procédure pour accès temporaire) : 1° à réception d'une demande, émission d'un mandat par un juge d'instruction, sur accord du Procureur ; 2° exécution du mandate et obtention des données demandées auprès de la personne morale/physique concernée qui les détient. (Serv Sec) En tant *qu'Etat requérant* : 1° envoi de la demande au Bureau du Procureur général (General Prosecutor's Office - GPO) ; 2° vérification par celui-ci qu'elle respecte les obligations légales nationales et internationales ; 3° envoi de la demande (dans les dix jours) par le GPO à l'Etat requis, via les canaux diplomatiques ou autres. En tant *qu'Etat requis* : 1° à réception de la demande, examen des conditions légales par le GPO, et identification des services répressifs compétents pour l'exécution ; 2° des mesures sont prises par le service répressif compétent durant un mois (ou plus si nécessaire) pour exécuter la demande, et les données sont transmises au GPO ; 3° envoi de la réponse (données obtenues ou raisons pour	(Serv Sec) En tant *qu'Etat requérant* : – la confidentialité des résultats d'enquêtes entreprises par l'accès à un système informatique sans l'accord de son propriétaire (« enquêtes sous couverture ») entraîne une procédure complexe pour leur transfert à un Etat étranger ; – Délai court (1 mois) En tant *qu'Etat requis* : – différences entre les législations.

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	lesquelles la demande n'a pu être exécutée) par le GPO à l'Etat requérant.	
Royaume-Uni	En tant *qu'Etat requérant* : dépend des conditions dans l'Etat requis. Le caractère de nécessité et la proportionnalité de la demande sont évalués par les autorités nationales. En tant *qu'Etat requis* : [Problème : Référence à un "lien plus bas" [à clarifier]]	En tant qu'Etat *requérant* : – [manque d'informations sur] le fait de savoir si les données ont été conservées et sont disponibles ; – temps pris pour obtenir les données. En tant *qu'Etat requis* : problèmes de terminologie ; divergences dans le vocabulaire juridique utilisé.
États-Unis d'Amérique	En tant *qu'Etat requérant* : 1° soumission, par l'autorité d'enquête ou de poursuite demandant les données, d'un projet de demande au Bureau des affaires internationales (Office of International Affairs - OIA) ; 2° examen et rectification éventuelle de la demande par l'OIA ; 3° après vérifications légales, l'OIA approuve la demande, la signe et la transmet directement à l'autorité centrale de l'Etat requis. En tant *qu'Etat requis* : 1° révision de la demande par l'OIA, pour déterminer si les données sont conservées et si la base légale et factuelle est suffisante pour les obtenir ; (Mesures supplémentaires : conservation des données si cela n'est pas déjà fait ; si la base légale et factuelle n'est pas suffisante, discussion et demande d'informations supplémentaires.) 2° transmission de la demande au bureau du Procureur fédéral compètent pour obtenir une injonction du tribunal ; 3° délivrance d'une injonction du tribunal et production des données ; 4° examen de la qualité des données pour répondre à la demande et transmission à l'Etat requérant par les canaux	En tant *qu'Etat requérant* : – retards dans l'exécution de la demande ; – lacunes dans les lois de l'Etat requis ; – manque de connaissances/formation de l'autorité centrale de l'Etat requis sur des questions high-tech ; – manque de personnel dans l'Etat requis ; – méconnaissance de l'importance croissance de la preuve électronique, et d'une réaction appropriée à cette évolution. En tant *qu'Etat requis* : – retards dans les envois de l'Etat requérant (lorsque la conservation n'a pas été requise, il est à craindre que les données aient été détruites lorsque la demande arrive) ; – manque de connaissance des conditions nationales pour l'obtention de preuves ; – non-respect des conditions nationales ; – lenteur des autorités nationales à exécuter les demandes (surcharge).

Pays	Procédure pour l'envoi/la réception de demandes (Q 2.4)	Problèmes rencontrés (Q 2.5)
	utilisés pour les DEJ.	

4 Évaluation des canaux et moyens de coopération

4.1 Autorités, canaux et moyens de coopération

Le Chapitre III de la Convention de Budapest ne remplace pas d'autres accords ou arrangements bi- ou multilatéraux relatifs à la coopération internationale qu'une Partie a contractés, mais au contraire encourage le recours à ces accords et arrangements pour ce qui est de la coopération en matière de cybercriminalité et de preuve électronique :

> Article 23 – Principes généraux relatifs à la coopération internationale
>
> Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Les Parties doivent donc recourir à ces accords et arrangements pour les demandes d'entraide concernant des données informatiques stockées :

> Article 31 – Entraide concernant l'accès aux données stockées
>
> 2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

La plupart des États autorisent donc différentes autorités à s'appuyer sur l'accord utilisé dans un cas spécifique. Ainsi, 36 Parties à la Convention de Budapest sont Parties à la Convention européenne sur la coopération en matière pénale (STE 30)[18], et 28 sont Parties au 2e Protocole additionnel à ce traité (STE 182)[19]. Ce protocole permet, entre autres, une coopération directe entre les autorités judiciaires :

> Article 4 – Voies de communication
>
> L'article 15 de la Convention est remplacé par les dispositions suivantes:
>
> «1. Les demandes d'entraide judiciaire, ainsi que toute information spontanée, seront adressées, sous forme écrite, par le Ministère de la Justice de la Partie requérante au Ministère de la Justice de la Partie requise et renvoyées par la même voie. Toutefois, elles peuvent être adressées directement par l'autorité judiciaire de la Partie requérante à l'autorité judiciaire de la Partie requise et renvoyées par la même voie. »

---

[18] http ://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=030&CM=8&DF=&CL=ENG
Les Parties à la STE 30 comptent également le Chili et Israël qui ont été invités à adhérer à la Convention de Budapest. En outre, la Corée est Etat Partie et le Brésil et l'Afrique du Sud ont été invités à adhérer.

[19] http ://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG
Les Parties à la STE 182 comptent également le Chili et Israël qui ont été invités à adhérer à la Convention de Budapest.

En vertu de l'article 6 STE 182, les Parties doivent déclarer quels sont les autorités qui sont des autorités judiciaires pour elles. Bon nombre de Parties ont ainsi défini toute une palette d'autorités judiciaires, notamment les ministères de la Justice, services de poursuite et tribunaux, mais aussi souvent les autorités d'enquête[20].

En l'absence de tels accords et arrangements, les Parties à la Convention de Budapest appliquent les procédures prévues à l'article 27[21] et, conformément aux dispositions de celui-ci, désigne également des autorités centrales pour l'emploi et la réception de demandes d'entraide.

Les réponses au questionnaire indiquent que certains États autorisent de multiples canaux, d'autres suivants en revanche une approche plus limitée :

- canaux diplomatiques : Australie, Philippines, Ukraine.
- ministère de la Justice : Albanie, Turquie.
- Bureau du Procureur General : Arménie, République dominicaine.
- Multiples canaux : Belgique, Bosnie-Herzégovine, Bulgarie, Croatie, Finlande, Géorgie, Lettonie, Lituanie, Roumanie, Suisse, «l'ex-République yougoslave de Macédoine».

L'article 25.3 permet des moyens de communication accélérée en cas d'urgence :

> Article 25 – Principes généraux relatifs à l'entraide
>
> 3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

Les réponses au questionnaire suggèrent que l'utilisation du courriel ou des fax n'est pas limitée aux cas urgents mais est acceptée en toutes circonstances par la plupart des Parties. Certains exigent qu'une documentation écrite formelle soit soumise en plus.

Conclusions préliminaires :

- les voies et autorités pour des demandes effectuées en vertu de l'article 31 devraient être utilisées de manière flexible et pragmatique. Les Parties devraient clarifier de manière large quelles voies et autorités sont acceptées pour ce type de demande.
- Les contacts directs devraient être privilégiés.

---

[20] http ://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=182&CM=8&DF=03/11/2013&CL=ENG&VL=1

[21] Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

- Une plate-forme en ligne donnant la liste des autorités centrales et judiciaires et des conditions à remplir serait utile.

- Les autorités centrales et points de contact 24/7 devraient donner des conseils concernant les autorités pertinentes pouvant être contactées directement dans un État Partie.

4.2 Demandes urgentes/réponses accélérées

L'article 31 prévoit des réponses selon la procédure accélérée à des demandes d'entraide :

> Article 31 – Entraide concernant l'accès aux données stockées
>
> 3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:
>
> a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou
>
> b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Les Parties appliquent différents critères pour considérer une demande comme « urgente ». Une demande est considérée urgente si elle concerne :

- un danger imminent pour la vie et la santé, des préjudices matériels substantiels, une attaque imminente à l'encontre d'infrastructures critiques ou cas similaires : Albanie, Belgique, Bosnie-Herzégovine, Estonie, Finlande, Allemagne, Pays-Bas, Norvège, Serbie, Slovénie, Espagne, Turquie, Royaume-Uni, États-Unis ;

- un risque de perte ou de modification de données : Autriche, Bosnie-Herzégovine, Chypre, France, Allemagne, Lettonie, Moldova, Norvège, Roumanie, Slovaquie, Espagne, Suisse, Turquie, Ukraine, États-Unis ;

- toute demande concernant une infraction liée à la cybercriminalité : Croatie ;

- d'autres considérations (par exemple un délai très court, la nature de l'infraction, la conservation en cours, la prévention d'un crime spécifique) : Australie, Costa Rica, Géorgie, France, Italie, Moldova, Portugal, Roumanie, Finlande.

Un certain nombre de Parties indique qu'elles évaluent l'urgence des demandes au cas par cas (Estonie, Géorgie, Lituanie).

Pour des demandes urgentes, bon nombre de Parties ont mis en place des mécanismes, des procédures ou des canaux spécifiques, par exemple:

- recours aux points de contact 24/7, officiers de liaison, réseaux judiciaires (notamment EUROJUST et le Réseau judiciaire européen), les canaux de coopération policière (avec aussi INTERPOL) et similaire : Albanie, Australie, Autriche, Belgique, Bosnie-Herzégovine, Bulgarie, Chypre, République dominicaine, Estonie, Finlande, France, Lettonie, Lituanie, Pays-Bas, Portugal, Roumanie, Serbie, Slovaquie, Slovénie, Espagne, Turquie, États-Unis.

- communication directe par téléphone, courriel ou fax, y compris un contact préalable avec les autorités étrangères pour les alerter d'une demande imminente : Albanie, Australie, Costa Rica, Géorgie, Allemagne, Roumanie, Serbie, Espagne, Suisse.

- contact direct avec les autorités judiciaires étrangères : Autriche, Belgique, Slovaquie.

- priorité aux demandes portant la mention « urgente »: Albanie, Hongrie, Roumanie, et Espagne.

- autres arrangements : en Norvège, lorsqu'elle est Etat requis, un Procureur délivré un mandat de perquisition ou de production sans accord du tribunal, si la demande justifie l'urgence.

4.3 Rôle des points de contact 24/7

En vertu des dispositions de l'article 35, les Parties établissent des points de contact 24/7 « afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. »

L'article 35 ne spécifie pas un rôle pour les points de contact 24/7 en matière de demandes d'entraide relevant de l'article 31, mais ne l'exclut pas non plus, et l'article 35.2.b prévoit que :

> 2.b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

La question 3.2.1 portait donc sur la compétence des points de contact 24/7 en matière de demande d'entraide, la question 3.2.2 concernant, quant à elle, la coordination des points de contact avec les autorités compétentes pour l'entraide afin d'accélérer l'exécution des demandes en vertu de l'article 35.2.b.

Les points de contact d'environ la moitié des États qui ont répondu au questionnaire sont compétents pour envoyer ou recevoir des demandes d'entraide. Certains d'entre eux peuvent servir de canal de transmission seulement (tel est le cas de la Bosnie-Herzégovine, de l'Estonie, de la Hongrie et des Pays-Bas).

D'autres peuvent également délivrer des commissions rogatoires ou exécuter (ou superviser ou participer à l'exécution) des demandes d'entraide (Costa Rica, Chypre, Finlande, Géorgie, Lituanie, Norvège, Roumanie, Serbie, «l'ex-République yougoslave de Macédoine», Royaume-Uni).

Certains pays (Albanie, Arménie, Australie, Autriche, Bulgarie, Estonie, Japon, Pays-Bas, Roumanie, Slovaquie) ont signalé une communication directe et une liaison régulière entre les points de contact 24/7 et les autorités chargées de l'exécution des demandes d'entraide.

Dans un certain nombre d'États, toutefois, il semble qu'il y ait un risque de déconnexion entre les points de contact et les autorités chargées des demandes d'entraide. Par exemple, les points de contact ne sont pas informés lorsque des demandes de conservation sont suivies par une demande d'entraide ; il arrive également qu'aucune disposition pratique n'ait encore été établie en ce qui concerne la coordination accélérée entre les points de contact et les autorités chargées des demandes d'entraide.

Conclusion préliminaire :

- Les points of contact 24/7 – à moins qu'ils ne puissent, de leur propre autorité, envoyer, recevoir ou exécuter des demandes d'entraide relevant de l'article 31 - devraient avoir la capacité de faciliter l'exécution accélérée des demandes d'entraide.

Etat	**Compétence pour l'envoi/la réception de demandes**
Albanie	OUI
Arménie	NON
Australie	NON
Autriche	NON
Azerbaïdjan	OUI
Belgique	NON
Bosnie-Herzégovine	OUI (transmission par les canaux d'INTERPOL ; recours à Eurojust)
Bulgarie	NON
Costa Rica	OUI
Croatie	NON
Chypre	OUI
Estonie	OUI (transmission seulement)
Finlande	OUI (pour des affaires relevant de sa compétence)
France	NON
Géorgie	OUI
Allemagne	NON
Hongrie	OUI (transmission seulement)
Japon	NON
Lettonie	NON
Lituanie	OUI
Moldova	NON
Monténégro	OUI [à confirmer]
Pays-Bas	OUI (transmission seulement)
Norvège	OUI
Philippines	OUI (transmission seulement)
Portugal	NON
Roumanie	OUI
Serbie	OUI
Slovaquie	NON (mais facilite la transmission)
Slovénie	Sert de canal pour la transmission
«l'ex-République yougoslave de Macédoine»	OUI
Turquie	NON
Royaume-Uni	NON
Royaume-Uni	OUI
États-Unis d'Amérique	NON (mais facilite la transmission)

4.4 Contact direct pour obtenir des données émanant de personnes physiques ou morales dans des juridictions étrangères

Pour ce qui concerne la possibilité de contacter des détenteurs de données (personnes physiques ou morales telles que des fournisseurs de services sur Internet) dans des juridictions étrangères directement pour obtenir des données stockées, un petit nombre d'États considère que ceci n'est pas autorisé dans leur droit interne, alors que dans la majorité des autres, cela n'est ni régulé ni autorisé.

En pratique, les services de police de nombreux États contactent directement des fournisseurs de services étrangers[22]. Lorsque ceux-ci ont une représentation légale sur le territoire de l'autorité requérante, les demandes peuvent prendre la forme d'une injonction de produire relevant du droit interne, même si les données sont physiquement stockées à l'étranger. Dans certains cas, les autorités répressives ont des accords avec des fournisseurs de services étrangers.

Les fournisseurs de services étrangers peuvent répondre positivement à une demande sous certaines conditions, par exemple :

- la divulgation de données doit être autorisée dans le droit interne du pays du fournisseur de services (les fournisseurs américains sont autorisés à divulguer des données relatives au trafic ou sur l'abonné, mais par des données relatives au contenu), faute de quoi des sanctions administratives ou pénales peuvent être encourues.

- La demande doit être légale (autrement dit, il faut une injonction de produire).

- La demande doit avoir un lien avec la juridiction de l'autorité requérante (par exemple elle doit concerner des personnes ou des adresses IP sur le territoire de l'autorité requérante).

En outre, certains fournisseurs ont établi des procédures spécifiques pour répondre à des demandes en urgence (par exemple menace sur la vie et la santé).

Il ressort des réponses que fréquemment, les informations ainsi obtenues ne peuvent être utilisées comme preuve dans une procédure judiciaire et qu'il conviendrait qu'elles soient formalisées par la suite au moyen d'une demande d'entraide en bonne et due forme.

4.5 Coordination dans des affaires internationales complexes

Pour ce qui est des mécanismes permettant de coordonner des affaires internationales complexes, les États citent :

- le recours à EUROPOL, EUROJUST ou INTERPOL ;

---

[22] Les rapports de transparence de sociétés telles que Facebook, Google, Microsoft ou Yahoo montrent qu'au moins la moitié des Parties à la Convention de Budapest soumettent des demandes. Dans la presque totalité des cas, elles concernent des données relatives aux abonnés ou au trafic.
https ://www.microsoft.com/Environ/corporatecitizenship/en-us/reporting/transparency/
https ://www.google.com/transparencyreport/?hl=en-US
http ://l.yimg.com/pj/info/tr/Yahoo_Transparency_Report-Jan-juin-2013-1.3.pdf
https ://www.facebook.com/Environ/government_demandes

- l'établissement d'équipes communes d'enquête (parfois, il faut pour cela des accords en vigueur) ;
- le recours à des officiers de liaison ou réseaux de services répressifs.

Conclusion préliminaire :

- Il peut être utile d'envisager d'inclure une disposition sur les équipes communes d'enquête dans un Protocole à la Convention de Budapest similaire à l'article 20 de la STE 182[23].

[23] http ://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=182&CM=8&DF=&CL=ENG

4.6 Tableaux concernant les questions 3.1 – 3.4**

4.6.1 Autorités (Question 3.1.1)

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
Albanie	ministère de la Justice, Bulevardi Zog. I., Tirana	ministère de la Justice, Bulevardi Zog. I., Tirana Bureau central national d'Interpol, Bulevardi Deshmoret e Kombit, Tirana	Service chargé de la cybercriminalité, ministère de l'Intérieur Tirana, Albanie
Arménie	Service principal pour la lutte contre le crime organisé, Police, Arménie	Service principal pour la lutte contre le crime organisé, Police, Arménie	Division sur High-tech Crime, Service principal pour la lutte contre le crime organisé, Police, Arménie
Australie	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australie	International Crime Cooperation Central Authority Attorney-General's Department 3-5 National Circuit Barton ACT 2600 Australie	AOCC Watchfloor Operations Australian Federal police GPO Box 401 Canberra ACT 2601 Australie
Autriche	*Bundesministerium für Justiz* (ministère fédéral de la Justice) Abt. IV 4 *Internationale Strafsachen* (Affaires criminelles internationales) 1070 Wien, Museumstrasse 7 Tel. : +43 1 52 1 52-0 E-Mail : team.s@bmj.gv.at	*Bundesministerium für Justiz* (ministère fédéral de la Justice) Abt. IV 4 *Internationale Strafsachen* (Affaires criminelles internationales) 1070 Wien, Museumstrasse 7 Tel. : +43 1 52 1 52-0 E-Mail : team.s@bmj.gv.at z	*Bundesministerium für Inneres* (ministère fédéral de l'Intérieur) *Bundeskriminalamt* (Bureau fédéral de la police criminelle) Büro 5.2 Cyber-Crime-Compétence-Center Josef Holaubek Platz 1 1090 Wien
Azerbaïdjan	ministère de la Sécurité nationale 2, Parliament Avenue, Baky, AZ 1006, Azerbaïdjan ; e-mail : secretoffice@mns.gov.az	ministère de la Justice 1, Inshaatchilar Avenue, Baky, AZ 1073, Azerbaïdjan ; e-mail : contact@justice.gov.az	Service de lutte contre les délits en matière de communications et la cybercriminalité ministère de la Sécurité nationale

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
Belgique	Service Public Fédéral Justice Service de la coopération internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	Service Public Fédéral Justice Service de la coopération internationale pénale Boulevard de Waterloo 115 1000 Bruxelles Fax : +32(0)2/210.57.98	Service fédéral chargé de la cybercriminalité
Bosnie-Herzégovine	ministère de la Justice of Bosnie-Herzégovine	ministère de la Justice of Bosnie-Herzégovine	Direction pour la coordination des organes de la police de Bosnie-Herzégovine (coopération policière internationale - Interpol)
Bulgarie	ministère de la Justice (étape judiciaire), Bureau du Procureur (étape pré-judiciaire)	ministère de la Justice (extradition), Bureau du Procureur (arrestations provisoires et gardes à vue)	Service National de lutte contre le crime organisé, relevant du ministère de l'Intérieur
Croatie	ministère de la Justice de la Croatie Vukovarska Street 49 10 000 Zagreb	ministère de la Justice de la Croatie Vukovarska Street 49 10 000 Zagreb	ministère de l'Intérieur, Police – Direction de la police criminelle, Ilica 335, 10 000 Zagreb
Chypre	ministère de la Justice et de l'Ordre public Athalassas Av. 125 1461 NICOSIA	ministère de la Justice et de l'Ordre public Athalassas Av. 125 1461 NICOSIA	Bureau pour la lutte contre la cybercriminalité et Police scientifique, Commissariat central de Chypre ministère de la Justice et de l'Ordre public Athalassas Av. 125 1461 NICOSIA
Danemark	ministère de la Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Danemark	ministère de la Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Danemark	Police nationale danoise, Service de Police, Polititorvet 14, DK-1780 Copenhagen V, Danemark
République dominicaine	Procuradoria General de la Republica et Service d'enquête pour la criminalité High Tech (DICAT), Police nationale	Procuradoria General de la Republica et Service d'enquête pour la criminalité High Tech (DICAT), Police nationale	Service d'enquête pour la criminalité High Tech (DICAT), Police nationale, Santo Domingo, République dominicaine
Estonie	ministère de la Justice	ministère de la Justice	Bureau du Renseignement criminel, Service

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
			de police criminelle
Finlande	ministère de la Justice, Eteläesplanadi 10, FIN-00130 Helsinki	Pour demandes d'extradition, ministère de la Justice, Eteläesplanadi 10, FIN-00130 Helsinki Pour demandes d'arrestation provisoire, Bureau National d'Investigation, Jokiniemenkuja 4, FIN-01370 Vantaa	Bureau National d'Investigation, Affaires internationales/Centre de communication
France	Des autorités judiciaires françaises à des autorités judiciaires étrangères, transmission par le ministère de la Justice (*ministère de la Justice, 13, Place Vendôme, 75042 Paris Cedex 01*) D'autorités judiciaires étrangères aux autorités judiciaires françaises, transmission par les canaux diplomatiques (*ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*)	ministère des Affaires étrangères pour extradition (*ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*) ; Le Procureur territorialement compétent pour les demandes d'arrestation provisoire	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication" (11, Rue des Saussaies, 75800 Paris)
Géorgie	ministère de la Justice de Géorgie 24a Gorgasali str. Tbilissi 0114 - Géorgie Tel : +995322405143 - Fax : +995322405142 E-mail : international.psg@justice.gov.ge	ministère de la Justice de Géorgie 24a Gorgasali str. Tbilissi 0114 - Géorgie Tel : +995322405143 Fax : +995322405142 E-mail : international.psg@justice.gov.ge	Unité Cybercriminalité ministère de l'Intérieur de Géorgie Service de police criminelle 10 G. Gulua str. Tbilissi 0114 - Géorgie
Allemagne	ministère des Affaires étrangères: Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	ministère des Affaires étrangères : Auswärtiges Amt, Werderscher Markt 1, 10117 Berlin	Unité nationale chargée des crimes High Tech, Bureau fédéral de la police criminelle 65193 Wiesbaden
Hongrie	Avant d'entamer une procédure pénale : International Loi Enforcement Cooperation Centre Budapest, Teve u. 4-6 1139 - Hongrie Après le démarrage d'une procédure pénale : Ministère public hongrois	ministère de la Justice pour extradition ou arrestation provisoire. Bureau central national d'Interpol pour les arrestations provisoires.	International Loi Enforcement Cooperation Centre, Police Alternative : Unité Criminalité High Tech Bureau National d'Investigations

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
	Budapest, Markó u. 4-6 1055 - Hongrie		
Islande	ministère de la Justice, Skuggasundi, 150 Reykjavík, Islande Tel.: +354 545-9000 Fax: +354 552-7340 Email: postur@irr.is	ministère de la Justice, Skuggasundi, 150 Reykjavík, Islande Tel.: +354 545-9000 Fax: +354 552-7340 Email: postur@irr.is	1- National Commissioner of the Icelandic Police (Ríkislögreglustjórinn), Skúlagata 21, 101 Reykjavík, Iceland 2- Ministry of the Interior, Department of Public Security
Italie	ministère de la Justice Département des affaires judiciaires Direction générale de la justice pénale Bureau II (Coopération judiciaire internationale) Viale Arenula 70 I - 00186 ROMA	ministère de la Justice Département des affaires judiciaires Direction générale de la justice pénale Bureau II (Coopération judiciaire internationale) Viale Arenula 70 I - 00186 ROMA	Servizio Polizia Postale e delle Comunicazioni ministère de l'Intérieur Alternative : Bureau du Procureur de district de Rome – Section Cybercriminalité
Japon	le Ministre de la Justice ou la personne qu'il a designée (Directeur de la Division des affaires internationales) et La Commission nationale pour la sécurité publique ou la personne désignée par la Commission (Directeur de la Division des opérations d'enquête internationales) Service du crime organisé Police nationale 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974	The Minister pour Foreign Affairs 2-2-1, Kasumigaseki Chiyoda-ku Tokyo 100-8919	Division des opérations d'enquête internationales Service du crime organisé Police nationale 2-1-2, Kasumigaseki Chiyoda-ku Tokyo 100-8974
Lettonie	ministère de la Justice Brivibas Blvd. 36, Riga LV-1536, Lettonie	Bureau du Procureur général Kalpaka Blvd. 6, Riga LV-1801, Lettonie	Service de la Coopération internationale du Département central de la police criminelle, Police de l'Etat Brivibas Str. 61, Riga LV-1010, Lettonie
Lituanie	ministère de la Justice et Bureau du	ministère de la Justice et Bureau du Procureur	Service de la Police relevant du ministère

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
	Procureur général de la Lituanie	général de la Lituanie	de l'Intérieur de la Lituanie
Malte	Bureau du Procureur général The Palace Valletta Malte Email : ag.mla@gov.mt	ministère de la Justice Bureau du Premier Ministre Auberge de Castille Valletta VLT 2000 Malte	Unité sur la cybercriminalité Police de Malte Siège de la Police Floriana Malte
Moldova	Bureau du Procureur Général - phase des poursuites pénales: 26, Banulescu - Bodoni str., MD-2012 Chisinau, République de Moldova. ministère de la Justice – phase judiciaire ou exécution de la peine: 82, 31 août 1989 str., MD-2012 Chisinau, République de Moldova.	Bureau du Procureur Général - phase des poursuites pénales: 26, Banulescu - Bodoni str., MD-2012 Chisinau, République de Moldova. ministère de la Justice – phase judiciaire ou exécution de la peine: 82, 31 août 1989 str., MD-2012 Chisinau, République de Moldova.	Service des technologies de l'information et des enquêtes en matière de cybercriminalité, Bureau du Procureur général: 26, Banulescu - Bodoni str., MD-2012 Chisinau, République de Moldova. Direction de la prévention et de la lutte contre la cybercriminalité, l'information et les infractions transnationales, ministère de l'Intérieur: 14, Bucuriei str., MD-2004 Chisinau, République de Moldova.
Monténégro	ministère de la Justice du Monténégro, adresse : Vuka Karadžica 3, 81 000 Podgorica	ministère de la Justice du Monténégro, adresse : Vuka Karadžica 3, 81 000 Podgorica Pour une mise en garde à vue en l'absence d'accord : NCB Interpol en Podgorica, adresse : Bulevar Svetog Petra Cetinjskog 22, 81 000	Inspecteur chargé de la lutte contre la cybercriminalité Direction de la Police du Monténégro
Pays-Bas	*Landelijk Parket van het openbaar ministerie* (Bureau national du ministère public) Postbus 395 3000 AJ ROTTERDAM	ministère de la Sécurité et de la Justice Bureau de l'entraide judiciaire internationale en matière pénale PO BOX 20301 2500 EH THE HAGUE	National High Tech Crime Unit (NHTCU)
Norvège	The National Criminal Investigation Service (KRIPOS)	ministère de la Justice et de la Police, P.O. Box 8005, N-0030 OSLO	Division criminalité High Tech National Criminal Investigation Service

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
			(KRIPOS)
Philippines	Ministère de la Justice		Ministère de la Justice –Bureau pour la cybercriminalité
Portugal	*Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal	*Procuradoria-Geral da República* (Rua da Escola Politécnica, 140 – 1269-269 Lisboa, Portugal)	1. Unité Cybercriminalité, Police Judiciare 2. Coordinateur des enquêtes criminelles au Portugal
Roumanie	Bureau du Procureur auprès de la Haute cour de Cassation pour les enquêtes préalables au procès (adresse : Blvd. Libertatii nr. 12-14, sector 5, Bucuresti) ministère de la Justice pour les demandes en cours de procès ou durant l'exécution de la peine ministère de la Justice, Direction du droit international et de la coopération judiciaire, Service chargé de la coopération judiciaire internationale en matière pénale, Apolodor Street non. 17, Sector 5, 050741	ministère de la Justice (adresse : Str. Apollodor nr. 17, sector 5, Bucuresti)	1. Service de lutte contre la cybercriminalité au sein de la Section de lutte contre le crime organisé et le trafic de stupéfiants, Haute cour de cassation et Justice (adresse : Blvd. Libertatii nr. 12-14, sector 5, Bucuresti). 2. Unité Cybercriminalité, Direction Générale de la lutte contre les drogues et la criminalité organisée
Serbie	Procureur de District pour le crime High Tech Savska 17A 11000 Beograd ministère de l'Intérieur de la Serbie Direction de la Police criminelle Service de lutte contre le crime organisé Bulevar Mihajla Pupina 2 11070 novi Beograd	Procureur de District pour le crime High Tech Savska 17A 11000 Beograd ministère de l'Intérieur de la Serbie Direction de la Police criminelle Service de lutte contre le crime organisé Bulevar Mihajla Pupina 2 11070 novi Beograd	Procureur de District pour le crime High Tech Savska 17A 11000 Beograd ministère de l'Intérieur de la Serbie Direction de la Police criminelle Service de lutte contre le crime organisé Bulevar Mihajla Pupina 2 11070 novi Beograd
Slovaquie	ministère de la Justice de la Slovaquie (Zupné námestie 13, 81311 Bratislava) et	ministère de la Justice de la Slovaquie (Zupné námestie 13, 81311 Bratislava) pour	Bureau National Central d'Interpol Vajnorská 25812 72 Bratislava Slovaquie

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
	Bureau du procureur général (Stúrova 2, 81285 Bratislava)	l'extradition Procureur compétent du Bureau régional du Procureur et ministère de la Justice pour réception de demandes pour des gardes à vues ministère de la Justice de la Slovaquie et Tribunal compétent pour délivrer un mandat d'arrêt international	
Slovénie	ministère de la Justice Zupanciceva 3 SI - 1000 Ljubljana	ministère des Affaires étrangères pour extradition : Presernova 25 SI - 1000 Ljubljana ministère de l'Intérieur, Direction de la Police d'enquête criminelle, section chargée de la coopération internationale policière pour les demandes de mise en garde à vue :	1 ministère de l'Intérieur, Direction de la Police d'enquête criminelle, section chargée de la coopération internationale policière 2 Alternative : Unité chargée des enquêtes en matière de cybercriminalité, Direction de la police criminelle
Espagne	Sous-Direction générale chargée de la coopération judiciaire internationale, ministère de la Justice San Bernardo 62, 28071, Madrid	Sous-Direction générale chargée de la coopération judiciaire internationale, ministère de la Justice San Bernardo 62, 28071, Madrid	1 Unité de la Police nationale chargée des enquêtes High Tech 2 Comisaria General de Policia Judicial, Brigada de Investigación Tecnológica (CGPJ), C/ Julián González Segador s/n 28071 Madrid
Suisse	Office fédéral de la Justice, Département Fédéral de la Justice et de la Police, 3003 Berne	Office fédéral de la Justice, Département Fédéral de la Justice et de la Police, 3003 Berne	Centre d'opérations FEDPOL Office fédéral de la Justice
« ex-République yougoslave de Macédoine »	ministère de la Justice	ministère de la Justice	Bureau du Procureur Skopje

Pays	Autorité en matière de DEJ en l'absence d'autres traités (article 27)	Autorité en matière d'extradition et d'arrestation provisoire en l'absence d'autres traités (article 24)	Point of contact 24/7 (article 35)
Turquie			Département cybercriminalité, Police turque nationale
Ukraine	ministère de la Justice de l'Ukraine (pour ce qui concerne la justice) et Bureau du Procureur Général de l'Ukraine (pour les organes chargés de l'enquête pré-judiciaire)	ministère de la Justice de l'Ukraine (pour ce qui concerne la justice) et Bureau du Procureur Général de l'Ukraine (pour les organes chargés de l'enquête pré-judiciaire)	Division de lutte contre la cybercriminalité, ministère de l'Intérieur
Royaume-Uni	Pour des affaires concernant l'Angleterre, le Pays de Galles et l'Irlande du Nord : Royaume-Uni Central Authority Home Office, 5th Floor Peel building 2 Marsham Street London, SW1P 4DF Concernant l'Ecosse: International Co-operation Unit Argyle House C Floor 3 Lady Loison Street Edinburgh, EH3 9DR Concernant la fiscalité indirecte: Law Enforcement & International Advisory Division HM Revenue et Customs – Solicitor's Office, Room 2/74 100 Parliament Street London, SW1A 2BQ	Home Office Judicial Co-operation Unit 5th Floor, Fry building 2 Marsham Street London SW1P 4DF Scottish Government (lorsqu'on présume que la personne se trouve en Ecosse) Criminal Procedure Division St. Andrew's House Regent Road Edinburgh EH1 3DG	National Cyber Crime Unit, National Crime Agency
3. États-Unis	Office of International Affairs, États-Unis Department of Justice, Criminal Division, Washington, D.C., 20530		Computer Crime et Intellectual Property Section (CCIPS) U.S. Department of Justice, Washington, DC

4.6.2 Voies, méthodes et moyens de coopération (Question 3.1)

3.1.2 Quels voies, procédures et moyens (fax, courrier électronique ou autre) de coopération utilisez-vous généralement pour demander par la voie de l'entraide des données informatiques stockées dans un autre Etat ? 3.1.3 Quels sont les critères pour considérer une demande comme « urgente » ? 3.1.4 En tant qu'Etat requérant : utilisez-vous des mécanismes, procédures ou canaux différents si vous considérez que votre demande est « urgente » ? 3.1.5 En tant qu'Etat requis : utilisez-vous des mécanismes, procédures ou canaux différents pour exécuter une demande considérée comme « urgente » ?

Pays	**Voies, méthodes et moyens (Q 3.1.2)**	**Demandes urgentes (Q 3.1.3-3.1.5)**
Albanie	*Voie* : habituellement le ministère de la Justice. *Moyens et méthodes* : fax, email ou par écrit.	*Critères* : toute indication d'urgence ; urgence spécifiée dans la demande (par exemple danger imminent pour la vie ou la santé de personnes ; préjudice matériel substantiel) *Utilisation de mécanismes, procédures ou canaux spécifiques* - En tant qu'Etat requérant, utilisation des canaux disponibles les plus efficients (point de contact étranger 24/7 ; communication directe par e-mail ou fax) - En tant qu'Etat requis, les demandes urgentes sont prioritaires ; contact direct par téléphone ou email).
Arménie	*Voie* : Bureau du Procureur Général *Moyens et méthodes* : e-mail, fax, téléphone	Indication d'urgence : mention « urgente » sur la demande.
Australie	*Voie* : Canaux diplomatiques. *Moyens et méthodes* : - version papier de la demande d'entraide par la valise diplomatique, porteur et lettre recommandée ; - des versions électroniques sont également envoyées par e-mail	*Critères* : dépend des faits d'espèce (délai urgent du tribunal ou de l'enquête ; nature de l'infraction). *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant :

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
	(lorsque les contacts sont déjà établis dans le pays étranger).	- contact avec les autorités étrangères pour les alerter d'une demande d'urgence imminente et leur donner brièvement les détails de son contenu ; - Envoi d'une version électronique de la demande (en général par email) signée par le délégué du procureur général. - Utilisation du réseau de liaisons internationales de la police fédérale pour veiller à la bonne réception de la demande et à une réaction rapide. En tant qu'Etat requis : - à condition que suffisamment d'informations soient communiquées, contact avec les forces répressives pour les alerter et mettre en place les moyens nécessaires, en attendant la demande
Autriche	*Voie* : n/a. *Moyens et méthodes* : tout moyen permettant une transmission rapide, en particulier le fax et le courrier électronique	*Critères* : risque de perte de données (étant donné que dans certains pays la période de stockage est courte) ; données utilisées comme base pour des mesures d'enquête supplémentaire (par exemple, le gel de preuves) *Utilisation de mécanismes, procédures ou canaux spécifiques* - dans le réseau UE, Eurojust et EJN ; - contact direct entre autorités judiciaires.
Azerbaïdjan	Tous les canaux sont acceptables.	
Belgique	Tous les canaux sont acceptables.	*Critères :* - risque pour la vie d'une personne ou son intégrité physique - attaque imminente contre une infrastructure critique Canaux : coopération policière et contacts directs.
Bosnie-Herzégovine	*Voies* : ministère de la Justice (ou ministère des Affaires étrangères, le cas échéant) accords bilatéraux internationaux avec la Serbie, la Croatie, le Monténégro, l'ex-République yougoslave de Macédoine et la Slovénie (affaires pénales).	*Critères* : infractions pénales qui peuvent avoir des conséquences graves (par exemple terrorisme, meurtre, kidnappings) ; situation de risque pour la vie de personnes ; raison de craindre une altération ou destruction de preuves numériques ; autres demandes identifiées

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
	et accords assumés par succession INTERPOL ; Eurojust ; points de contact 24/7 *Moyens et méthodes* : Téléphone et email.	comme « urgentes ». *Utilisation de mécanismes, procédures ou canaux spécifiques* INTERPOL, quand cela est prévu par le traité.
Bulgarie	*Voie* : entraide par le biais des autorités compétentes (et coopération policière par le biais d'Europol, Interpol, les officiers de liaison et le Centre SELEC). *Moyens et méthodes* : courrier postal, fax et courrier électronique. Les autorités nationales peuvent demander la certification de l'authenticité du matériel employé et la transmission des originaux.	*Critères* : lorsque l'État requérant l'a indiqué comme urgent *Utilisation de mécanismes, procédures ou canaux spécifiques* Possibilité d'utiliser le canal Interpol, ainsi que le Réseau judiciaire européen, EUROJUST, les officiers consulaires et les officiers de liaison dans les ambassades.
Costa Rica	*Moyens et méthodes* : divers moyens de communication, en particulier des informations scannées envoyées par courrier électronique, fax et porteur lorsque la demande est urgente	*Critères* : si l'État requérant a indiqué sur la demande « urgent », en tenant compte des circonstances de l'affaire particulière (type d'infraction ; caractéristiques des victimes et de leurs implications etc.). *Utilisation de mécanismes, procédures ou canaux spécifiques* : En tant qu'Etat requérant, utilisation de mécanismes préliminaires pour contacter l'État requis (y compris l'envoi de demande via courrier électronique) et obtenir des informations sur les conditions à remplir. En tant qu'Etat requis, les autorités nationales souhaitent un traitement rapide des documents (envois de copies numériques de documents ; utilisation de livraison par porteur pour répondre à la demande).
Croatie	*Voie* : Interpol. *Moyens et méthodes* : lettre, fax, e-mail	*Critères* : toute demande concernant un cyber délit *Utilisation de mécanismes, procédures ou canaux spécifiques* : - En tant qu'Etat requérant : non. - En tant qu'Etat requis : non.
Chypre	*Moyens et méthodes* : par fax, email, courrier postal et, en cas d'urgence, par les canaux d'Interpol/Europol	*Critères :* si l'enquête en est à un point tel qu'il est nécessaire d'obtenir les données stockées pour conclure l'enquête, ainsi que lorsque l'enquête a été terminée et que l'affaire est en jugement

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		devant la justice, les données informatiques étant alors nécessaire pour être présentées comme preuve au tribunal. *Utilisation de mécanismes, procédures ou canaux spécifiques* : non. Cependant, en fonction de l'urgence de l'affaire, les canaux du Réseau judiciaire européen et d'Eurojust peuvent être utilisés.
République dominicaine	*Voie :* procureur général	Il est possible de recourir aux officiers de liaison représentés dans le pays (FBI, Services secrets).
Estonie	*Moyens et méthodes* : habituellement par email (crypté si nécessaire)	*Critères* : approche cas par cas. Principaux motifs : rétention de données, commission en cours d'une infraction ou prévention d'une infraction imminente ; prévention de perte financière ; protection de la vie ; demande marquée « urgente ». *Utilisation de mécanismes, procédures ou canaux spécifiques* Marquage de la demande comme « urgent ». Utilisation du réseau 24/7 et/ou des systèmes de communication de données d'Interpol et d'Europol.
Finlande	*Voies* : canaux diplomatiques, contact direct, Interpol et Europol. *Moyens et méthodes* : fax, email, courrier postal.	*Critères* : Si une personne a été arrêtée durant l'enquête et est en garde à vue dans ce contexte ; si les menaces graves ou danger pour la vie humaine, atteinte grave aux biens ou à l'environnement etc. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : Voir Q 3.1.2. Une exécution rapide est demandée. En tant qu'Etat requis : recours à l'exécution rapide et au mécanisme Eurojust 24/7.
France	*Moyens et méthodes* : Email (par une boîte de messagerie spéciale)	*Critères* : conservation en cours, risque important que des données soient altérées ou effacées. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requis/requérant : points de contact 24/7, lorsqu'ils sont disponibles.
Géorgie	*Voies* : canaux établis par des accords internationaux, canaux	*Critères* : examen au cas par cas, basé sur la motivation raisonnable

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
	diplomatiques, et autres canaux directs. *Moyens et méthodes* : la version papier écrite est privilégiée pour des questions de validité. Le fax, le courrier électronique ou autres méthodes sont autorisés.	de l'urgence par l'État requérant (en particulier en cas de délais courts dans ses procédures judiciaires). *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : mention sur la demande « urgent ». Le MJ justifie cette mention et peut envoyer une copie scannée de la demande d'entraide par courrier électronique. En tant qu'Etat requis : démarrage accéléré de toutes les mesures nécessaires pour exécuter la demande ; mention « urgent » sur la demande et contacte des services répressifs nationaux ; prompte information de l'État requérant lorsque l'exécution ne peut pas être réalisée dans les délais souhaités
Allemagne	*Moyens et méthodes* : livraison par porteur ou email, en fonction de l'urgence	*Critères* : garde à vue en cours, prescription imminente, risque de perte de données (expiration de la durée de conservation provisoire des données), risque pour la santé et l'intégrité physique *Utilisation de mécanismes, procédures ou canaux spécifiques* transmission de la demande par avance par courrier électronique
Hongrie	*Moyens et méthodes :* E-mail, fax.	Les mêmes méthodes sont utilisées en général, mais, en tant qu'État requis, des dispositions sont prises pour obtenir les données immédiatement.
Islande	Email et fax sont suffisants afin de commencer l'exécution d'une demande et de gagner du temps. Neanmoins, les orginaux doivent suivre repidement par courrier.	Cela dépend des cas spécifiques. Par exemple, les demandes concernant un danger imminent pour la vie et la santé des gens ou un dommage méteriel conséquent sera toujours considéré comme priorité. Et aussi en s'appuyant les délais de justice ou d'enquête ou encore de la nature de l'infraction. En tant qu'Etat requis : la requête est traitée de manière prioritaire à tous les niveaux (Ministère, DDP et au niveau de la police)
Italie	Cela dépend des procédures habituellement acceptées par l'Etat requis.	*Critères* : Lorsque cela est nécessaire pour arrêter un crime en cours de commission *Utilisation de mécanismes, procédures ou canaux spécifiques*

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		non.
Japon	*Voies* : autorités centrales en vertu des traités sur l'EJI. *Moyens et méthodes* : courrier électronique international (EMS).	*Critères* : n/a. Pas d'utilisation de mécanismes, procédures ou canaux spécifiques. note : en tant qu'Etat requis, les demandes doivent être adressées aux autorités centrales pour des raisons d'efficience.
Lettonie	*Voies* : police de l'Etat et Bureau du Procureur Général. *Moyens et méthodes* : courrier ordinaire.	*Critères* : la demande concerne des données volatiles. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requis/requérant : contact direct et utilisation des officiers de liaison pour dupliquer et faciliter l'exécution de la demande.
Lituanie	*Voie* : le canal établi au sein du Bureau du procureur. *Moyens et méthodes* : emails.	*Critères* : pas de critères spécifiques. Examen au cas par cas. *Utilisation de mécanismes, procédures ou canaux spécifiques* Réseau 24/7.
Moldova	*Voie* : le canal établi au sein du Bureau du procureur. *Moyens et méthodes* : emails.	*Critères* : - réel danger que les preuves puissent être perdues ou détruites ; commission possible d'infractions supplémentaires ; - critères utilisés pour déterminer le temps raisonnable nécessaire pour résoudre l'affaire (complexité de l'affaire, conduite de procédure, importance du processus pour la personne concernée, victime mineure etc.)
Monténégro	Manque d'expérience.	*Critères* : n/a. *Utilisation de mécanismes, procédures ou canaux spécifiques* n/a.
Pays-Bas	*Voie* : dépend de la priorité donnée à la demande. *Moyens et méthodes* : e-mail et téléphone.	*Critères* : dépend de la demande ; des intérêts vitaux ou personnels doivent être concernés *Utilisation de mécanismes, procédures ou canaux spécifiques* téléphone, et parfois rencontre face à face.

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		Contact par le point de contact unique.
Norvège	Email au point de contact pertinent (pour commencer).	*Critères* : gravité de l'infraction, possibilité de perte de preuves vitales, risque de morts (par exemple, menace à la bombe). *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : oui et non. Utilisation des canaux habituels, mais suivi avec contact téléphonique. En tant qu'Etat requis : oui. Les procureurs peuvent délivrer un mandat de perquisition de production sans accord préalable du tribunal. Il est souhaitable de donner des informations détaillées sur le degré d'urgence (délai, etc.).
Philippines	*Voie :* canaux diplomatiques par lettre officielle de demande.	Les critères pour qu'une demande soit considérée comme « urgente » et les procédures dépendraient de l'accord bilatéral particulier sur l'entraide conclu entre les Philippines et le pays concerné.
Portugal	*Voie* : n/a. *Moyens et méthodes* : tous systèmes de communication, prioritairement courrier électronique	*Critères* : détention ou emprisonnement en cours, ou question liée à la liberté des personnes ; affaires indiquées comme urgentes par l'autorité compétente ; actes liés à la libération conditionnelle. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : points de contact 24/7, ainsi que les Points de référence centraux nationaux Interpol-G8. En tant qu'Etat requis : Utilisation des canaux du G8.
Roumanie	*Voie* : directement à l'autorité judiciaire requise, ou par l'autorité centrale (en fonction de l'instrument applicable). L'officier national auprès d'Eurojust est contacté pour faciliter l'exécution de la demande. *Moyens et méthodes* : envois par courrier dans tous les cas. Fax et email pour accélérer le processus.	*Critères* : la personne est en garde à vue ou des enquêtes doivent être menées ; un mandat d'arrêt européen doit être délivré ; délai fixé pour la rétention des données (six mois) ; risque de corruption et de disparition des preuves numériques. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : envoi des demandes par fax et email. Contact direct, si possible, avec la personne exécutant la demande. Spécification du délai applicable et du fait que le mis en cause est en garde à vue. Implication de l'officier national Eurojust.

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		En tant qu'Etat requis : l'exécution de la demande est prioritaire. Lorsqu'elles participent à l'exécution, les autorités requérantes peuvent recevoir des copies des documents et preuves confisqués.
Serbie	*Canaux* : habituellement par le biais du ministère de la Justice. *Moyens et méthodes* : n/a.	*Critères* : tout signe d'urgence ; urgence spécifiée dans la demande (danger imminent pour la vie et la santé de personnes ; endommagement substantiel de matériel). *Utilisation de mécanismes, procédures ou canaux spécifiques* - En tant qu'Etat requérant, utilisation des voies les plus efficientes disponibles (point de contact 24/7 étranger ; communication directe par email ou fax). - En tant qu'Etat requis, les demandes urgentes sont prioritaires ; contact direct par téléphone ou email.
Slovaquie	Pour des affaires non urgentes, l'email normal est utilisé ; pour des affaires urgentes, les demandes peuvent être envoyées par Interpol, fax, email, sous réserve de conditions prévues dans le traité international applicable.	Les demandes en vertu de l'article 29 sont urgentes (en tenant compte de l'objectif consistant à rendre les données disponibles en vue d'une demande d'entraide ultérieure et du risque possible de pertes des données). Pas de règles internes prescrites/élaborées pour trancher sur le caractère « urgent » d'une demande. Bien entendu, un délai de conservation peut justifier l'urgence d'une demande. De manière générale, l'évaluation du degré d'urgence d'une demande se fait au cas par cas. Le degré d'urgence d'une demande est déterminé soit par la possibilité de pertes de données (la période de stockage de données est susceptible d'expirer dans peu de temps), soit par la gravité de l'infraction ou l'impact des données sur l'affaire criminelle, ou encore du simple fait qu'un mis en cause est en garde à vue etc. En tant qu'Etat requérant : en cas de demande urgente, il est possible d'utiliser un moyen de communication ou de transmission moderne. Dans ce cas, il est possible de recourir à la communication directe avec des homologues pour s'assurer que tout se passe dans les

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		temps. Le recours aux canaux d'Interpol et autres canaux sécurisés est également envisageable. En tant qu'Etat requis : les mécanismes, procédures et canaux sont essentiellement déterminés par l'Etat requérant. En conséquence, en tant qu'Etat requis, nous pouvons envisager différentes options uniquement s'il est nécessaire d'obtenir des informations supplémentaires ou de communiquer davantage. Tous les moyens disponibles peuvent être utilisés.
Slovénie	*Voie* : habituellement, canaux Interpol et Europol. *Moyens et méthodes* : n/a.	*Critères* : situation constituent une menace pour la vie, la sécurité nationale, menace publique de haut niveau. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : utilisation des points de contact 24/7 prévus par la Convention sur la cybercriminalité. En tant qu'Etat requis : expérience insuffisante.
Espagne	*Moyens et méthodes* : habituellement par courrier postal.	*Critères* : temps écoulé depuis les faits (problèmes d'effacement de données, délai de prescription pour l'infraction), importance du délit objet de l'enquête, indication « urgente » par l'Etat requérant etc. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : envoi préalable de la demande par email et/ou fax ; utilisation des points de contact du RJE, IbeRed, et son système de communication Iber@. En tant qu'Etat requis : priorité aux demandes urgentes ; liaison avec l'Etat requérant.
Suisse	*Voie* : Interpol, Europol pour la coopération policière ; canaux diplomatiques pour les emails normaux. *Moyens et méthodes* : fax, e-mail, puis demande formelle par écrit. Les messageries électroniques sécurisées sont souvent	*Critères* : danger imminent de perte/effacement de données ; une réponse est attendue dans les 24 heures (standard d'Interpol). *Utilisation de mécanismes, procédures ou canaux spécifiques* - entraide : non.

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
	utilisées (SIENA d'Europol)	- Coopération policière : (requérant) possibilité d'indiquer que la demande est « urgente » avec information des autorités compétentes –email, téléphone). (Requis) – priorité aux demandes urgentes.
«l'ex-République yougoslave de Macédoine»	Canaux : Accord avec la Serbie, la Croatie, le Monténégro et la Bosnie-Herzégovine sur les affaires de criminalité organisée et de corruption (et autres affaires pénales). Sous certaines conditions, un contact direct est possible entre procureurs. Moyens et méthodes : Essentiellement emails.	Critères : demandes demandant une réponse dans les 24 heures. Utilisation de mécanismes, procédures ou canaux spécifiques - En tant qu'Etat requérant : pas de mécanismes spécifiques ; la demande est marquée « urgente ». - En tant qu'Etat requis : pas de mécanismes spécifiques.
Turquie	*Voie* : ministère de la Justice. *Moyens et méthodes* : par écrit, fax et emails.	*Critères* : crimes graves, situation avec risque pour la vie de personnes, délai de conservation. *Utilisation de mécanismes, procédures ou canaux spécifiques* - En tant qu'Etat requérant : utilisation d'INTERPOL et points de contact 24/7, par fax, email ou téléphone. - En tant qu'Etat requis : utilisation de mécanisme de point de contact, par fax, email ou téléphone.
Ukraine	(MdI) *Voie* : Canaux diplomatiques. *Moyens et méthodes* : Téléphone, email. (Serv. Sec.) *Moyens et méthodes* : par courrier postal uniquement, conformément au droit national.	(MdI) *Critères* : demande pour la conservation de données pouvant servir de preuves électroniques, les données étant très volatiles. *Utilisation de mécanismes, procédures ou canaux spécifiques* non. (Serv Sec) *Critères* : pas de critères. Fonction de la situation spécifique et de la demande. *Utilisation de mécanismes, procédures ou canaux spécifiques* - En tant qu'Etat requérant : - En tant qu'Etat requis : possible, exceptionnellement, de recevoir des demandes par email, fax, etc., avant réception officielle par

Pays	Voies, méthodes et moyens (Q 3.1.2)	Demandes urgentes (Q 3.1.3-3.1.5)
		courrier.
Royaume-Uni	*Moyens et méthodes* : habituellement par la poste, à moins qu'il existe des services de fax ou de emails sécurisés.	*Critères* : lorsqu'une personne est en garde à vue ou va être libérée ; risque immédiat pour les personnes ; risque de disparition d'actifs. *Utilisation de mécanismes, procédures ou canaux spécifiques* En tant qu'Etat requérant : marquage de la demande « urgente », avec justification de cette mention et informations complémentaires. En tant qu'Etat requis : l'autorité centrale traite la demande aussi rapidement que possible. Des critères spécifiques s'appliquent (justification de l'urgence, délai, suivi lorsque l'entraide n'est plus nécessaire).
États-Unis d'Amérique	*Voie* : autorités centrales (en cas conservation, autorités centrales ou réseau 24/7). *Moyens et méthodes* : moyens accélérés, y compris fax ou email.	*Critères* : menaces à l'encontre d'infrastructures importantes ; affaires concernant des enfants ; danger significatif de poursuite d'actes criminels ; destruction de données ou fuite d'un suspect. *Utilisation de mécanismes, procédures ou canaux spécifiques* Large utilisation des canaux 24/7. Transmission de demandes par voie électronique, ou avant que leur traduction ne soit disponible (accord de l'Etat requis). Contacts étroits par téléphone ou email. note : la transmission électronique de demandes n'est pas limitée aux cas urgents.

4.6.3 Rôle des points de contact 24/7 (Question 3.2)

3.2 Rôle des points de contact 24/7 en matière d'entraide (relation entre les articles 35 et 31 de la Convention de Budapest) 3.2.1 Votre point de contact 24/7 est-il habilité à envoyer ou recevoir une demande d'entraide ? Si oui, veuillez expliquer quel est son rôle, y compris dans l'exécution de la demande. 3.2.2 Si le point de contact 24/7 n'est pas compétent en matière d'entraide, veuillez expliquer comment il agit en coordination avec les autorités compétentes dans ce domaine selon une procédure accélérée (article 35.2b). Veuillez décrire la relation entre les deux services et la manière dont la coopération pourrait être améliorée afin d'accélérer l'exécution des demandes d'entraide.

Pays	**Compétence pour faire une demande d'entraide (Q 3.2.1)**	**Coordination avec les autorités chargées de l'entraide (Q 3.2.2)**
Albanie	*Compétence* : oui. *Rôle* : envoyer et recevoir des demandes, communication, échange des données et des conseils juridiques avec d'autres PC. Le PC communique avec des FSI et autres personnes juridiques et transmets directement les données obtenues.	*Améliorations* : remplacement de la commission rogatoire par des demandes électroniques ; possibilité pour les PC d'envoyer/recevoir directement une demande, avec notification au ministère de la Justice pertinent.
Arménie	*Compétence* : non. Celle-ci relève du Bureau du Procureur général *Rôle* : le point de contact 24/7 peut uniquement exécuter des demandes d'entraide sans conditions spécifiques.	Si une demande est « urgente », elle peut être envoyée via le point de contact 24/7, mais une demande d'entraide sera exigée pour obtenir les informations demandées. Si le PC 24/7 de la police lance une demande d'entraide, la police fait appel au Bureau du Procureur général.
Australie	*Compétence* : non, mais le point of contact peut apporter une assistance policière aux pays étrangers en attendant une demande formelle.	Bonne relation de travail et liaison régulière en ce qui concerne les DEJ.
Autriche	*Compétence* : non, mais le point of contact sert d'intermédiaire avec les services de poursuite et peut transmettre une demande à l'autorité nationale compétente.	Communication directe et informelle entre le point de contact 24/7 et les autorités charges de l'exécution. Pas de retards dus à cette coordination.
Azerbaïdjan	Compétence : Oui. Le point de contact peut fournir une assistance spécialisée, ordonner une conservation rapide des données	

Pays	Compétence pour faire une demande d'entraide (Q 3.2.1)	Coordination avec les autorités chargées de l'entraide (Q 3.2.2)
	informatiques ou des données de trafic, après l'obtention d'une décision de justice la saisie d'objets contenant des données et effectuer ou faciliter l'exécution des documents de procédures	
Belgique	non.	Ces procédures ne sont pas encore en place.
Bosnie-Herzégovine	*Compétence* : oui, par les canaux d'Interpol *Rôle* : transmettre la demande d'entraide en cas d'urgence.	n/a.
Bulgarie	*Compétence* : non.	Très bonne coopération avec les autorités chargées des DEJ, rendue nécessaire par le fait que le point de contact est la seule unité du pays spécialisée en cybercriminalité. Si l'autorité chargée des DEJ transmet une demande au point de contact, celui-ci peut faire conserver les preuves électroniques et les obtenir.
Costa Rica	*Compétence* : oui. Le point de contact est chargé des procédures en matière de coopération pénale internationale et est l'autorité centrale pour divers instruments internationaux sur l'entraide.	non applicable.
Croatie	*Compétence* : non.	Le PC envoie la demande au service compétent, qui procède aux vérifications nécessaires. L'enquête criminelle nécessaire qui est menée est coordonnée avec le Procureur compétent.
Chypre	oui. Le point de contact qui est le Chef de l'Unité Cybercriminalité peut accepter des DEJ et supervise leur exécution. Il a également la responsabilité d'en informer le MJPO.	non applicable.
Estonie	*Compétence* : oui, mais uniquement pour envoyer et recevoir des demandes.	Le point de contact 24/7 : - est compétent pour transmettre des informations aux services pertinents et trouver un destinataire compétent qui apporter son expertise, en-dehors des heures ouvrables si nécessaire ; - veille à ce que les informations soient transmises au décideur compétent.
Finlande	*Compétence* : oui, selon l'article 5 de la loi sur l'EJ. *Rôle* : Le point de contact peut faire une demande d'entraide et participe à l'exécution de demandes.	n/a. Voir Q 2.1. Si l'autorité n'est pas compétente, elle est tenue de la transmettre à l'autorité compétente.

Pays	Compétence pour faire une demande d'entraide (Q 3.2.1)	Coordination avec les autorités chargées de l'entraide (Q 3.2.2)
	En vertu de l'article 5 de la Loi générale sur les DEJ, une demande d'entraide peut être faite par le ministère de la Justice, un tribunal, un procureur ou un service d'enquête (police). Notre point de contact 24/7 est un représentant de la police (au NBI). En vertu de l'article 4 de la Loi générale sur les DEJ, les demandes d'entraide à la Finlande peuvent être adressées au ministère de la Justice ou directement à l'autorité qui est compétente pour l'exécuter. La Police a un grand rôle et de larges compétences en matière d'exécution de demandes d'entraide en Finlande lorsqu'elle agit en tant qu'autorité d'enquête.	
France	*Compétence* : non.	Pour ce qui est du gel de données, interaction entre le ministère de la Justice (Bureau d'entraide pénale internationale) et le point of contact 24/7 au sein du ministère de l'Intérieur. Pas d'informations sur le point de savoir si des demandes faites via le réseau 24/7 des points de contact font ensuite l'objet d'une demande d'entraide.
Géorgie	*Compétence* : oui. Le point de contact 24/7 peut envoyer/recevoir des demandes et entreprendre toutes les mesures nécessaires pour apporter l'assistance requise. Lorsqu'une demande relève de sa compétence, il l'adresse au ministère de la Justice.	n/a. Voir Q 3.2.1.
Allemagne	*Compétence* : non, mais le point de contact 24/7 peut faire en sorte que les données soient conservées par avance.	*Demandes entrantes* : le point de contact 24/7 peut organiser la conservation provisoire de données ; à réception de la demande, il peut entrer en contact de manière préliminaire avec l'Office fédéral de la Justice. *Demandes sortantes* : contact du service répressif compétent avec le point de contact 24/7, soit par avance, soit à l'initiative de l'Office fédéral de la justice une fois la demande reçue.
Hongrie	Le point de contact 24/7 est autorisé à envoyer/recevoir des	non applicable.

Pays	Compétence pour faire une demande d'entraide (Q 3.2.1)	Coordination avec les autorités chargées de l'entraide (Q 3.2.2)
	demandes d'entraide (il en assure la transmission)	
Islande	Non. tout es les rquêtes sont transférées au ministère	Le point de contact 24/7 contacte l'expert juridique au ministère
Italie	[	n/a.
Japon	*Compétence* : non.	Liaison du point de contact 24/7 avec l'autorité centrale compétente, par emails et téléphone si nécessaire.
Lettonie	*Compétence* : le point de contact 24/7 envoie et reçoit, échange des données et suit les requêtes de conservation des données. Le point de contact a les pouvoisr d'un institut de renseignement (il peut vérifier n'importe quel type de donnée ou bien le point de contact peut faire suivre une demande à l'institution compétente si les sujets des requêtes ou les actions sont sophistiqués	Contacts directs entre la Police nationale et le Bureau du Procureur général.
Lituanie	*Compétence* : oui. Le point de contact 24/7 peut directement envoyer/recevoir, exécuter et suivre des demandes de conservation de données.	non applicable (Voir Q 3.2.1)
Moldova	*Compétence* : non.	- Activités du Procureur, des enquêteurs et officiers concernés par des affaires de cybercriminalité dans le même bâtiment ; - utilisation de modes de communication urgents.
Monténégro	*Compétence* : oui. *Rôle* : envoyer et recevoir des demandes d'entraide.	n/a.
Pays-Bas	*Compétence* : oui, le point de contact 24/7 peut envoyer/recevoir des demandes d'entraide ; ce canal est rarement utilisé. En cas d'urgence, le réseau 24/7 peut être utilisé pour recevoir des demandes en avance.	Préparation de la demande par l'équipe chargée de la criminalité high-tech, qui envoie le projet au Bureau du Procureur national, lequel finalise la demande, qui est ensuite signée par un Procureur.
Norvège	*Compétence* : oui. Le point of contact a des contacts parmi les officiers de police, procureurs et à Interpol. L'Autorité nationale de poursuite se trouve dans le même bâtiment.	non applicable.
Philippines	Uniquement par le biais du ministère de la Justice.	Le MJ est l'autorité compétente en matière de demandes d'entraide.
Portugal	*Compétence* : non.	Le point de contact a la compétence légale pour exécuter des demandes urgentes visant la conservation de données. Il transmet immédiatement les demandes formelles ainsi que d'autres mesures en-dehors de sa compétence au Service du Procureur afin

Pays	Compétence pour faire une demande d'entraide (Q 3.2.1)	Coordination avec les autorités chargées de l'entraide (Q 3.2.2)
		qu'elles soient exécutées de manière accélérée.
Roumanie	*Compétence* : oui. Le point de contact peut apporter une assistance spécialisée, ordonner la conservation accélérée de données informatiques ou relatives au trafic, ainsi que la saisie d'objets contenant des données, et exécuter ou faciliter l'exécution des commissions rogatoires.	Coopération directe entre le point de contact et l'Office chargé de la coopération internationale au sein du DIICOT ; les procureurs des deux instances travaillent ensemble sur des demandes complexes.
Serbie	*Compétence* : oui. *Rôle* : - envoyer et recevoir des demandes, communiquer, échanger des données et des conseils juridiques avec d'autres PC ; - communiquer avec des FSI et autres personnes morales et transmettre directement les données obtenues.	*Améliorations* : remplacement de la commission rogatoire par des demandes électroniques ; possibilité pour les PC d'envoyer/recevoir directement une demande, avec notification au ministère de la Justice pertinent.
Slovaquie	Le point de contact 24/7 est le Bureau National d'Interpol, qui est le canal à même de faciliter la transmission d'une demande.	Le Bureau National d'Interpol est en contact direct avec le Bureau du Procureur général. Le service de poursuite est organisé hiérarchiquement. En Slovaquie, il y a un système de procureurs d'astreinte (24/7).
Slovénie	*Compétence* : oui. - les points de contact 24/7 reçoivent des demandes de toutes les unités de police, les traduisent et les envoient à l'Etat requérant ; - les points de contact 24/7 reçoivent des demandes étrangères et les transmettent à l'unité de police compétente.	non applicable.
Espagne	*Compétence* : oui. Il est compétent pour des mesures d'exécution uniquement dans des affaires de coopération policière.	Pas de réponses disponibles.
Suisse	n/a.	n/a.
«l'ex-République yougoslave de Macédoine»	*Compétence* : oui. *Rôle* : - envoyer et recevoir des demandes. - En tant que Procureur, le PC peut directement communiquer avec le juge d'instruction pour la délivrance d'une injonction de gel ou de saisie ; et communiquer par l'intermédiaire du MJ pour faire progresser l'entraide.	n/a.

Pays	**Compétence pour faire une demande d'entraide (Q 3.2.1)**	**Coordination avec les autorités chargées de l'entraide (Q 3.2.2)**
Turquie	*Compétence* : non.	Le PC soumet la demande à l'autorité centrale chargée des DEJ (ministère de la Justice) pour démarrer l'enquête en Turquie ou pour obtenir l'exécution de la demande via un Procureur ou par injonction d'un tribunal.
Ukraine	(MdI) *Compétence* : non. (Serv Sec) *Compétence* : non.	(MdI) Le point de contact ne participe pas à l'exécution des demandes d'entraide. (Serv Sec) - Le point de contact 24/7 peut uniquement échanger des informations opérationnelles ; - Absence de mécanisme spécifique pour partager des informations sur la cybercriminalité entre services pertinents.
Royaume-Uni	*Compétence* : oui.	non applicable.
États-Unis d'Amérique	*Compétence* : non (mais possibilité de transmettre les demandes effectuées par le canal des autorités centrales pour faciliter la coopération).	Notification des demandes par le point de contact 24/7 à l'autorité centrale. Possibilité pour le point de contact 24/7 d'aider l'autorité centrale à traiter des affaires difficiles, importantes ou urgentes.

4.6.4 Contact direct pour l'obtention de données auprès de personnes physiques ou morales (Question 3.3)

3.3 Contact direct pour obtenir des données auprès de personnes morales ou physiques

3.3.1 La législation de votre pays vous autorise-t-elle à contacter directement des détenteurs de données (comme des fournisseurs de services internet) dans des juridictions étrangères pour obtenir des données stockées ? Si oui :

- à quelles conditions ?
- pour quel type de détenteurs de données (fournisseurs de services internet, autres entités du secteur privé, personnes physiques) ?
- y a-t-il des différences selon le type de données demandées (abonné, trafic, contenu) ?

3.3.2 La législation de votre pays autorise-t-elle les services répressifs étrangers à contacter directement des détenteurs de données dans votre Etat ? Si oui :

- à quelles conditions ?
- pour quel type de détenteurs de données (fournisseurs de services internet, autres entités du secteur privé, personnes physiques) ?
- y a-t-il des différences selon le type de données demandées (abonné, trafic, contenu) ?

3.3.3 Si non, quelles sont les sanctions ?

Pays	**Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)**	**Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)**
Albanie	- Procureur : contact direct par le procureur autorisé pour tout type de détenteur de données. - Officiers de police judiciaire : contact direct autorisé, mais uniquement pour obtenir des renseignements concernant des abonnés. Solution possible : demander les données au représentant local du FSI.	Pas d'interdiction explicite dans le droit national. Une injonction de tribunal est exigée pour des données relatives au contenu. Sanction (lorsque les conditions préalables sur le plan national ne sont pas remplies) : le contact est qualifié en infraction.
Arménie	La loi n'empêche pas des contacts de ce type, mais l'exécution d'une demande dépend du FSI ou de l'entité qui la reçoit.	Possible en droit, mais la réponse dépend du FSI ou de l'entité.
Australie	Pas de fondement juridique spécifique en droit national. En pratique, les données sont demandées par le biais d'une DEJ, à moins que l'agence ne sache que le droit national applicable pour	Pas de fondement juridique en droit national, qui limite ce type d'action (les détenteurs de données peuvent être obligés de les remettre dans certains cas seulement).

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
	le FSI autoriserait une demande directe.	Sanction (pour le détenteur de données) : infraction passible d'une peine de prison pouvant aller jusqu'à 2 ans.
Autriche	En principe, non autorisé par la loi. En pratique, un contact direct pour éviter l'effacement de données n'a été pris qu'avec des FSI situés aux États-Unis (ce qui a été demandé par les autorités américaines elles-mêmes), avec des résultats positifs.	Pas de base légale Sanction : comportement qualifié comme violation de la souveraineté de l'Etat.
Azerbaïdjan	Le contact direct est normalement utilisé pour obtenir des informations relatives aux abonnées.	
Belgique	Pour le contenu, la coopération judiciaire est nécessaire. Il est possible de contacter des FSI directement s'il y a un accord avec le fournisseur (Google, Microsoft, Facebook). Ceci ne s'applique qu'aux données relatives à l'abonné et au trafic.	non. Si la procédure est illégale, les résultats obtenus ne peuvent être utilisés dans des procédures judiciaires.
Bosnie-Herzégovine	Pas de base légale claire. contact direct possible en pratique, en cas d'urgence ; une demande officielle doit absolument être envoyée par la suite.	Possible en pratique.
Bulgarie	Pas de base légale claire en droit national.	Pas de cadre juridique. Conformément au droit national, les personnes physiques ou morales peuvent être obligées de communiquer des informations, ou peuvent refuser de le faire. Des données relatives au contenu peuvent être fournies si elles proviennent ou affectent une personne physique ou morale, avec son consentement.
Costa Rica	n/a. Remarque générale : le droit national n'autorise pas l'application d'une loi étrangère.	n/a. Voir Q 3.3.1
Croatie	Pas de base légale En pratique : possible, sur la base de la Convention sur la cybercriminalité.	En principe : pas possible. Sanction : refus de la demande. En pratique : possible, sur la base de la Convention sur la cybercriminalité.
Chypre	pas possible	pas possible Procédure DEJ exigée.
Estonie	non réglementé en droit national. En pratique, les autorités nationales contactent bien des FSI étrangers.	non réglementé en droit national. Cependant, certains détenteurs de données y compris des FSI ne peuvent divulguer des données qu'aux

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
		autorités du pays. Sanction : violation du droit national entraînant des poursuites administratives.
Finlande	non réglementé en droit national. Peut relever de l'infraction pénale de violation des fonctions officielles par un agent public.	Voir Q 3.3.1.
France	non réglementé en droit national. En pratique, des requêtes judiciaires sont adressées à des FSI dans une juridiction étrangère (par exemple Facebook, Google) pour identifier des utilisateurs, lorsque le FSI n'a pas de bureau local ou est surchargé de demandes.	pas de base légale. Absence d'expérience pratique.
Géorgie	non réglementé en droit national. En pratique, il est possible d'obtenir des données de FSI et d'autres entités du secteur privé situées à l'étranger, avec leur consentement. Ces données peuvent servir de preuve en justice.	non réglementé en droit national. Sanction : dépend du type de données envoyées sans la permission des autorités nationales (l'envoi d'informations secrètes engage la responsabilité pénale ; l'envoi d'autres informations entraîne des sanctions administratives).
Allemagne	oui, à condition que le contact émane des autorités de poursuite et n'entraîne pas de mesures policières.	non. Sanction : n/a.
Hongrie	pas possible.	pas possible. Pas de sanctions prévues.
Islande	Non	Non. Pas prévu par la loi islandaise
Italie	Non autorisé en droit national.	non. Sanction : n/a.
Japon	Pas d'interdiction claire dans le droit national, mais un contact direct sans l'accord préalable de l'Etat concerné reviendrait à une violation de la souveraineté de l'Etat.	- non, en vertu du droit international (souveraineté de l'Etat) ; - Les FSI dans la juridiction nationale ne sont pas autorisés à divulguer à des services répressifs étrangers des informations relevant du secret des communications. Exception : nécessité ; délivrance d'une injonction d'un tribunal. Sanction : déterminée au cas par cas.
Lettonie	non. Le contact direct ne peut pas server à obtenir des preuves.	non.

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
		Sanction : dépend du type de données. Cela peut aller jusqu'à la responsabilité pénale pour divulgation illégale de données relatives au contenu/correspondance.
Lituanie	Pas d'interdiction en droit national, mais certaines conditions doivent être remplies. En pratique : le contact direct est habituellement utilisé pour obtenir des renseignements concernant des abonnés, ainsi que des données relatives au trafic et au contenu.	Pas d'interdiction au titre du droit national, mais les limites et interdictions applicables dans le pays doivent être respectées (informations concernant des secrets d'Etat, la vie privée et confidentielles etc.). Sanction : dépend du type d'infraction, la sanction peut être une amende ou une peine d'emprisonnement pouvant aller de deux à quinze ans.
Malte	Le droit national ne permet ni n'interdit de contacter des fournisseurs de services à l'étranger. Dans un certain nombre de cas, des fournisseurs de services étrangers ont été requis de fournir des données sur les abonnés et relatives au trafic directement à la Police de Malte. Selon le fournisseur de services contacté, les informations demandées sont fournies ou non directement au service répressif local. Des données relatives au contenu n'ont jamais été demandées directement à des fournisseurs de services étrangers.	Le droit national ne permet ni n'interdit à des services répressifs étrangers de contacter des fournisseurs de services situés dans le pays. La Police de Malte n'a pas connaissance de telles demandes. En règle générale, on s'efforce dans un premier temps d'obtenir les informations directement auprès des fournisseurs de services. Les demandes d'information sont suivies par le biais des canaux policiers ou de l'entraide si le contact direct n'a pas donné de résultats.
Moldova	non.	non. Considéré comme une violation de souveraineté. Sanction : annulation des preuves obtenues illégalement.
Monténégro	pas de base légale et manque d'expérience. Le contact direct est légalement possible, mais il n'est pas garanti que les preuves soient acceptées en justice.	contact direct possible en pratique.
Pays-Bas	Pas d'interdiction légale dans le droit national. Respect du droit national de l'Etat concerné.	non.
Norvège	non réglementé en droit national. En pratique : le contact direct est limité à des FSI spécifiques, essentiellement pour obtenir des renseignements concernant des abonnés ou pour geler des données en attendant une demande formelle.	- non, pour ce qui est informations et logs concernant les clients (obligation de secret) ; - oui, pour des renseignements concernant des abonnés, ainsi que d'autres type de données si le FSI consent à les remettre. Sanction (en cas de violation de la Loi sur la protection des données par un FSI national): peines d'amende ou de prison. Non pratiqué.

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
Philippines	Il y a eu des tentatives pour contacter directement des FSI dans une juridiction étrangère, mais qui n'ont rien donné.	non. Sanction possible en vertu de la loi n° 10173 ou de la Loi de 2012 sur la protection de la confidentialité des données.
Portugal	oui (pour tout type de données), lorsque (a) les données sont disponibles publiquement, ou (b) la personne légalement autorisée à divulguer les données y consent légalement et librement. Certaines conditions peuvent trouver à s'appliquer (en particulier, délivrance d'une injonction judiciaire).	oui (pour tout type de données), dans les mêmes situations que décrites en Q 3.3.1.
Roumanie	oui, conformément aux dispositions permettant d'obtenir directement des renseignements concernant des abonnés et logs auprès de Google et Facebook. Les données obtenues ne peuvent pas être utilisées comme preuves sans une demande ultérieure d'entraide juridique.	non, pour des raisons de souveraineté nationale. Sanction : n/a.
Serbie	Aucun obstacle légal en droit national. - Procureur : contact direct autorisé, pour tout type de détenteur de données et toutes données. - Officiers de police judiciaire : contact direct autorisé, mais uniquement pour obtenir des renseignements concernant des abonnés. Ainsi, il y a quelques années, contact direct avec Facebook n'a pas donné de résultat. Autres actions par les canaux d'Interpol.	Aucune interdiction explicite en droit national. Une injonction de tribunal est exigée pour des données relatives au contenu. Sanction (lorsque les conditions préalables dans le pays ne sont pas remplies) : le contact est qualifié d'infraction.
Slovaquie	non. Bien qu'il ne soit pas strictement interdit de demander directement des données à des détenteurs dans une juridiction étrangère, l'utilisation de ces données comme preuve poserait en revanche problème. Selon notre législation, les preuves émanant de l'étranger doivent être demandées via une DRJ.	Il s'agit d'une question complexe. En principe, si l'on ne présume pas de l'implication/n'implique pas les autorités officielles slovaques, il serait possible d'obtenir ces données en Slovaquie. Toutefois, nous pensons que cette possibilité est très hypothétique et ne s'appliquerait que dans des affaires très simples. On ne peut pas demander des données sans avertir de l'application d'une sanction ou pénalité au cas où le détenteur des données ne les communique pas volontairement. Dans le même temps, un certain nombre de données sont protégées par le secret bancaire ou le secret des télécommunications, ou encore par la législation de protection des données. Dans ce cas, elles ne peuvent être divulguées que dans le respect des conditions prévues par les lois de la Slovaquie. C'est pourquoi,

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
		en principe, des données stockées en Slovaquie ne peuvent être demandées aux fins de poursuites pénales que par le biais d'une DEJ. S'il y a violation des dispositions relatives au secret des télécommunications, secret bancaire ou autres règles de protection des données, une sanction administrative, voire pénale, peut s'appliquer. Il convient de noter que le principe de légalité s'applique en Slovaquie. L'obtention de données selon la procédure décrite ci-dessus pourrait avoir des conséquences négatives en matière d'admissibilité de la preuve.
Slovénie	non autorisé dans le droit national.	non autorisé dans le droit national. Sanction : diverses amendes pécuniaires, comme prévu dans la loi sur les communications électroniques.
Espagne	non.	non. Sanction : pas de sanction en tant que telle. Les preuves/données recueillies ne seront pas valides ou admissibles, et les services répressifs n'ont pas compétence pour obtenir des données par mesure contraignante.
Suisse	- non autorisé dans le droit national ; - autorisé en vertu de l'article 32.b de la Convention sur la cybercriminalité.	- non autorisé dans le droit national ; - autorisé en vertu de l'article 32.b de la Convention sur la cybercriminalité Sanction (lorsque l'article 32.b n'est pas applicable) : infraction pénale, punissable d'une peine d'amende ou d'emprisonnement pouvant aller jusqu'à 3 ans.
«l'ex-République yougoslave de Macédoine»	Le contact direct n'est pas interdit, même si l'expérience dans ce domaine concerne essentiellement Facebook.	non. [à clarifier]
Turquie	Pas d'interdiction explicite dans le droit national. Cela peut dépendre de l'existence d'accords pertinents entre États. En pratique, des données sont régulièrement demandées par contact direct. Des données obtenues sans demande d'entraide ont peu de chance d'être acceptées dans des procédures judiciaires, en vertu d'une	Pour ce qui est des données relatives au trafic et données relatives au contenu, le contact direct n'est pas possible (il faut une injonction de tribunal, ou en cas de danger, l'accord du Procureur public). Sanction : les données ne devraient pas être acceptées comme preuves dans des procédures judiciaires.

Pays	Contact direct de services répressifs avec des personnes physiques/morales dans une juridiction étrangère (Q 3.3.1)	Contact direct de services répressifs étrangers dans la juridiction nationale (Q 3.3.2 – 3.3.3)
	décision de la Cour suprême de Turquie sur l'application de la Loi 2992.	
Ukraine	(MdI) pas de base légale en droit national. Le contact direct n'est pas utilisé dans la pratique. (Serv Sec) pas de base légale en droit national.	(MdI) Pas d'interdiction claire en droit national, avec certaines restrictions (loi sur la protection des données personnelles ; secret d'Etat). Sanction (lorsque les restrictions ne sont pas respectées) : responsabilité pénale. (Serv Sec) pas de base légale en droit national. Sanction (lorsque les restrictions ne sont pas respectées) : responsabilité pénale.
Royaume-Uni	oui. Les seules conditions sont celles posées par l'Etat requérant.	oui, si le détenteur légal des données choisit de le faire. Sanction : aucune.
États-Unis d'Amérique	oui, si cela est autorisé par l'Etat étranger et dans les limites de ce qui semble acceptable à ce dernier.	oui. - en particulier avec des FSI, qui peuvent volontairement accepter de divulguer des données relatives au trafic et sur l'abonné (les données relatives au contenu ne peuvent pas être divulguées directement) ; - aussi avec d'autres personnes physiques/morales, à condition que les autorités nationales en soient notifiées. Sanction : pas d'expérience. Éventuellement, refus d'aider l'Etat demandeur à obtenir une copie des preuves qui puisse être utilisée au tribunal.

4.6.5 Coordination dans des affaires complexes (Question 3.4)

Les réponses au questionnaire concernaient les mécanismes suivants pour coordonner des affaires complexes nécessitant une action concertée (par exemple des perquisitions) dans plusieurs États :

Pays	Mécanismes pour la coordination d'affaires complexes
1. Albanie	Habituellement dans le cadre d'organisations de police telles qu'INTERPOL.
2. Arménie	La division de la police chargée des crimes high-tech est disponible pour coordonner au niveau national les affaires internationales complexes.
3. Australie	À réception d'une demande, liaison entre la police fédérale et des officiers au niveau national et à l'étranger (grâce à un réseau étendu d'officiers de liaison internationaux).
4. Autriche	Mécanismes de coordination mis en place par l'autorité centrale, ainsi qu'EUROJUST et les points de contact du Réseau judiciaire européen.
5. Azerbaïdjan	
6. Belgique	Équipes communes d'enquête.
7. Bosnie-Herzégovine	Mécanismes de DEJ.
8. Bulgarie	- Le Bureau du ministère public chargé de la cassation peut établir des équipes communes d'enquête avec d'autres états, composé de procureur et enquêteurs. Un accord entre les autorités compétentes des états participant doit être signé (activités, durée et composition des équipes) ; - entraide ; - coordination avec les officiers de liaison.
9. Costa Rica	Le droit national permet des travaux conjoints de recherche auxquels participent le procureur général et diverses autorités de pays étrangers.
10. Croatie	Équipes communes d'enquête sur la base d'un traité international (art. 201. CPA) et via EUROJUST
11. Chypre	n/d
12. Estonie	- Concours de différents experts et spécialistes en cas de besoin ; - Coordination des forces de police sur tout le territoire (après réception d'une demande par les officiers de liaison du Bureau du renseignement criminel).
13. Finlande	Approche ad hoc, en fonction de la nature de l'affaire.
14. France	Réunions opérationnelles sur des objectifs spécifiques, via Europol ou Interpol.
15. Géorgie	Équipes communes de détection des crimes, ce qui permet une action concertée (par exemple des perquisitions).
16. Allemagne	Coordination de demande parallèle (par exemple mesures coercitives coordonnées) Eurojust, Réseau judiciaire européen, équipes communes d'enquête, communication directe entre procureurs
17. Hongrie	n/d
18. Italie	Les commissions rogatoires sont le seul mécanisme permettant une telle coordination.
19. Japon	Coopération internationale par le biais du réseau ICPO, canaux diplomatiques et autorités centrales compétentes au titre des accords applicables en matière de DEJ.
20. Lettonie	- European Cybercrime Centre (EC3), - équipes communes d'enquête ; - contacts directs ; - bureaux de liaison.
21. Lituanie	- Équipes communes d'enquête, accueillant des officiers étrangers lorsqu'un

Pays	Mécanismes pour la coordination d'affaires complexes
	accord est en vigueur.
22. Malte	
23. Moldova	- Équipes communes d'enquête, sur la base d'un accord entre États.
24. Monténégro	n/a.
25. Pays-Bas	n/a.
26. Norvège	-Pas de mécanismes spécifiques ; - Assistance d'Eurojust dans certains cas.
27. Philippines	Partage de renseignements et coopération avec les attachés de l'État étranger.
28. Portugal	Équipes communes d'enquête, établies par accord entre États.
29. Roumanie	- Utilisation du réseau Eurojust ; - Coordination de toutes les autorités nationales impliquées ; - implication des magistrats de liaison et officiers de liaison dans les ambassades accréditées ; - Création d'équipes communes d'enquête.
30. Serbie	Habituellement dans le cadre d'organisation de police, comme EUROPOL et INTERPOL
31. Slovaquie	Le recours à Europol/Eurojust peut être envisagé comme solution pragmatique, même avec des pays hors de l'Union européenne.
32. Slovénie	Manque d'expérience suffisante.
33. Espagne	- Utilisation des réseaux Eurojust, au besoin ; - Coordination des mesures d'enquête, par liaison avec les autorités judiciaires étrangères.
34. Suisse	- Coordination de toutes les autorités impliquées par l'Office fédéral de justice ; - Coordination des enquêtes intercantonales et internationales par l'Office fédéral de police (Fedpol).
35. «l'ex-République yougoslave de Macédoine»	Absence de mécanismes spécifiques.
36. Turquie	- Activités (réunions, séminaires, projets conjoints, etc.) Avec des homologues pour partager des connaissances et discuter des problèmes ; - Signature de protocoles et d'accords avec des autorités centrales étrangères pour promouvoir la coopération ; - établissement de PC pour faciliter la communication entre autorités judiciaires ; - utilisation de canaux internationaux (INTERPOL, Centre SECI, EUROJUST et autres), ainsi que coopération avec les cellules de renseignements financiers étrangères.
37. Ukraine	ministère de l'Intérieur : décidé par chaque organe compétent. Pas de dispositions strictes réglementant cette question. Services de sécurité : équipes communes d'enquête (internationales) établies par le Bureau du procureur général.
38. Royaume-Uni	Utilisation de réseaux Eurojust, ou équivalent.
39. États-Unis d'Amérique	Beaucoup de travail, e-mail, appels téléphoniques, réunions si nécessaire.

5 Conclusions et recommandations

Comment on l'indiquait au départ, une entraide accélérée est l'une des conditions les plus importantes pour des mesures efficaces contre la cybercriminalité et d'autres infractions impliquant des preuves électroniques, étant donné la nature transnationale et volatile de ces dernières. En pratique, toutefois, les procédures liées à l'entraide sont jugées trop complexes, prenant trop de temps et mobilisant trop de ressources, et par là même étant par trop efficientes.

Le T-CY a donc procédé à une évaluation détaillée du fonctionnement de l'entraide, en se concentrant sur l'article 31 de la Convention de Budapest. L'évaluation se fonde sur les réponses de 36 États Parties et trois États observateurs. Des discussions ont eu lieu lors de la 9e Plénière (juin 2013), de la 10e Plénière (décembre 2013) et de la 11e Plénière (juin 2014) et la 12e Plénière, 2-3 décembre 2014 qui a adopté le présent rapport àl'unanimité.

Cette évaluation et les solutions proposées par les États qui ont répondu au questionnaire ont permis de dégager les conclusions et recommandations ci-après.

5.1 Conclusions

5.1.1 Conclusions générales

Concl 1 Le processus de demande d'entraide judiciaire (DEJ) est jugé inefficient en général, et en particulier pour ce qui concerne l'obtention de preuves électroniques. Il semble que les délais de réponse à une demande aillent de six à 24 mois. Bon nombre de demandes et donc d'enquêtes sont abandonnées. Ceci pénalise l'obligation positive des gouvernements de protéger la société et les personnes contre la cybercriminalité et d'autres crimes impliquant des preuves électroniques.

Concl 2 Or, les Parties semblent ne pas mettre pleinement à profit les opportunités offertes par la Convention de Budapest sur la cybercriminalité et par d'autres accords afin de parvenir à une entraide efficace en matière de cybercriminalité et de preuves électroniques.

Concl 3 On ne dispose pas de données ou de statistiques détaillées sur l'entraide. Il peut être utile d'établir des mécanismes pour suivre le processus de DEJ en ce qui concerne la cybercriminalité et les preuves électroniques.

5.1.2 Fréquence des demandes et types d'informations demandées

Concl 4 Pour ce qui est du type d'informations demandées, les informations concernant les abonnés ressortent comme étant les informations les plus fréquemment demandées. Le très grand nombre de demandes pour des données de ce type grève lourdement les autorités responsables du traitement et de l'exécution des DEJ, outre qu'il ralentit, voire empêche, les enquêtes criminelles. On pourrait donc penser que si l'on trouvait des solutions aux difficultés posées par les informations concernant les abonnés, les DEJ en seraient plus efficientes.

Concl 5 Les DEJ pour des preuves électroniques semblent le plus souvent liées aux fraudes et infractions financières, suivies par les crimes violents et crimes graves. Il s'ensuit que les DEJ pour accéder à des données informatiques stockées ne sont pas uniquement liées à la cybercriminalité (infractions commises à l'encontre et au moyen de systèmes informatiques – articles 2 à 11 de la Convention de Budapest), mais couvrent le recueil de preuves sous forme électronique lié à tout type d'infraction pénale.

Concl 6 La coopération policière est beaucoup plus fréquente que les DEJ. On peut partager énormément d'informations, mais elles doivent être validées avant de pouvoir être utilisées comme preuves en justice.

Concl 7 L'ouverture d'une enquête nationale à réception d'une DEJ, ou la transmission spontanée d'information, peuvent faciliter le partage d'informations sans DEJ ou accélérer cette dernière.

5.1.3 Procédures et conditions à remplir

Concl 8 Les conditions formelles à remplir et la législation applicable de l'État requis ne sont souvent pas connues ou pas respectées. Trop souvent, les demandes sont incomplètes ou trop vastes, ou encore ne respectent pas les seuils légaux ou le critère de la double incrimination. Il serait utile d'intensifier la formation, de communiquer davantage d'informations sur les conditions à remplir et d'utiliser des formulaires standardisés et plurilingues pour les demandes.

Concl 9 Il arrive que certains États refusent la coopération si l'affaire semble vénielle ou si elle représente une charge excessive pour l'État requis. Il faut davantage de transparence et de dialogue, si des seuils s'appliquent.

Concl 10 La question de la langue dans laquelle sont rédigées les demandes internationales d'entraide est un problème majeur, du fait des retards et des coûts que cela entraîne, ainsi que du fait de la qualité limitée des traductions. La plupart des États Parties acceptent des demandes rédigées en anglais.

5.1.4 Canaux et moyens de coopération

Concl 11 La plupart des Parties font usage de différents accords bilatéraux, régionaux et multilatéraux, ou s'appuient sur le principe de la réciprocité, et recourent à de multiples autorités et canaux de coopération tel que prévu dans la Convention de Budapest sur la cybercriminalité. Certains États, au contraire, adoptent une approche plus limitée et exigent que les demandes d'entraide soient transmises via les ministères de la Justice, un petit nombre seulement acceptant des demandes transmises par les canaux diplomatiques.

Concl 12 La possibilité d'une coopération directe avec les autorités judiciaires étrangères semble être sous-utilisée - hormis entre les États membres de l'UE. Cette utilisation limitée de l'option de coopération directe semble aussi s'appliquer pour des États non membres de l'UE qui sont pourtant Parties au Deuxième protocole additionnel à la Convention sur l'entraide en matière pénale (STE 182) du Conseil de l'Europe. Il pourrait être utile d'envisager des dispositions permettant une coopération directe entre les Parties à la Convention de Budapest.

Concl 13 Les États suivent des approches différentes s'agissant de décider si des demandes sont « urgentes ». Un nombre significatif d'États Parties traite une demande comme « urgente » s'il y a risque de perte ou de modification des données. En un tel cas, il est recouru aux points de contact 24/7, aux officiers de liaison, à des réseaux judiciaires ou à la coopération policière. Toutefois, il apparaît que des demandes ne sont pas toujours traitées selon la procédure accélérée, comme prévu à l'article 31.3 Convention de Budapest.

Concl 14 En vertu de l'article 35, les points de contact 24/7, s'ils ne sont pas eux-mêmes en mesure d'apporter l'entraide, devrait être capable de se coordonner avec les autorités responsables de l'exécution de la demande de manière accélérée. Si certains points de contact - en particulier lorsqu'ils sont de type poursuite - peuvent envoyer, recevoir et exécuter des demandes, et si

d'autres peuvent transmettre des demandes, dans l'ensemble, le rôle réel des points de contact 24/7 en matière d'entraide apparaît trop limité.

Concl 15 Les services de poursuite ou de police de nombreux États contactent des fournisseurs de services étrangers directement, en particulier ceux qui sont basés aux États-Unis, et ceux-ci peuvent répondre favorablement dans certaines conditions. Ces demandes peuvent prendre la forme d'injonctions nationales de produire des données. Certains fournisseurs peuvent répondre directement à des demandes en situation d'urgence. De manière générale, les conditions régissant des contacts directs de ce type ne sont pas claires ; dans certains pays, les informations ainsi obtenues peuvent devoir être validées par une demande d'entraide ultérieure avant de servir de preuve en justice.

Concl 16 L'établissement d'équipes communes d'enquête peut faciliter la coordination dans des affaires complexes. Les ECE peuvent être instauré sous réserve d'accord bilatéraux aux multilatéraux en vigueur. À l'heure actuelle, la Convention de Budapest ne prévoit rien spécifiquement concernant un tel mécanisme.

5.2 Recommandations

Ces recommandations pointent les mesures à prendre par les Parties sur le plan national et/ou les mesures à prendre par le T-CY et les programmes de renforcement des capacités.

Certaines recommandations peuvent devoirt faire l'objet d'un protocole additionnel. Toutefois, le présent rapport et ses recommandations ne doivent pas anticiper une décision sur l'élaboration d'un protocole.

5.2.1 Recommantions relevant de la responsabilité des autorités nationationales

Rec 1	Les Parties devraient pleinement mettre en œuvre et appliquer les dispositions de la Convention de Budapest sur la cybercriminalité, y compris les pouvoirs en matière de conservation (suite au rapport d'évaluation de 2012 du T-CY).
Rec 2	Les Parties devraient envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficience du processus d'entraide en ce qui concerne la cybercriminalité et les preuves électroniques.
Rec 3	Les Parties devraient envisager, pour l'entraide, d'affecter davantage de personnel et du personnel plus formé aux technologies, non seulement au niveau central mais aussi au niveau des institutions responsables de l'exécution des demandes (par exemple les Bureaux locaux des procureurs).
Rec 4	Les Parties devraient envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques. La formation et l'échange d'expériences devraient en particulier viser les procureurs et les juges et encourager une coopération directe entre autorités judiciaires. Une telle formation devrait être soutenue par les programmes de consolidation de capacités du Conseil de l'Europe et d'autres organisations.
Rec 5	Renforcer le rôle des points of contact 24/7 conformément à l'Article 35 Convention de Budapest, notamment : a. veiller, conformément à l'article 35.3 Convention de Budapest, à disposer de personnel formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir des activités liées à l'entraide ; b. veiller à ce que les points de contact promeuvent activement leur rôle de faire les autorités nationales et de leurs homologues étrangères ; c. assurer des réunions régulières et la formation du réseau 24/7 ; d. les autorités compétentes et les points de contact 24/7 devraient envisager des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et faire un retour d'information à l'Etat requérant e. établir, dans la mesure du possible, des points de contact (supplémentaires) dans les services de poursuite pour permettre un rôle plus direct en matière d'entraide et une réponse plus rapide aux demandes ; f. les points de contact 24/7 devraient jouer au moins un rôle de soutien pour les demandes "Article 31"
Rec 6	Les Parties devraient considérer la rationalisation des procédures et réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard Les Parties doivent partager les bonnes pratiques avec leT-CY.

Rec 7	Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.
Rec 8	Les Parties sont encouragées à établir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.
Rec 9	Les Parties devraient confirmer la réception des demandes systématiquement et notifier les actions prises.
Rec 10	Envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'informations ou accélérer l'entraide.
Rec 11	Les Parties devraient utiliser la transmission électronique des demandes, conformément à l'article 25.3 Convention de Budapest relatif à la divulgation rapide des moyens de communications.
Rec 12	Les Parties veillent à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.
Rec 13	Conformément à l'article 25.5 Convention de Budapest et au Paragraphe 259 du Rapport explicatif, les Parties sont encouragées à faire preuve de flexibilité lorsqu'elles appliquent la double incrimination qui faciliterait l'octroi de l'aide.
Rec 14	Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.
Rec 15	Les parties devraient assurer la transparence en ce qui concerne les conditions applicables en matière de demandes d'entraide, et les raisons de refus, notamment pour les seuils concernant les affaires vénielles, sur les sites Web des autorités centrales.

5.2.2 Les recommandations relevant de la responsabilité du T-CY

Rec 16	Le T-CY devrait faciliter une plus grande transparence vis-à-vis de la période de conservation des données suite à une demande de conservation étrangère conformément à l'article 29 de la Convention de Budapest. Le T-CY devrait documenter les périodes de conservation.

5.2.3 Les recommandations relevant prioritairement de la responsabilité des projets du Conseil de l'Europe en matière de renforcement des capacités

Rec 17	Le Conseil de l'Europe devrait – de part ses projets de renforcements des capacités - élaborer ou créer des liens vers des formulaires modèles standardisés, plurilingues pour les demandes de l'article 31.
Rec 18	Le Conseil de l'Europe devrait explorer la possibilité d'établir un fonds de ressources en ligne contenant des informations sur les systèmes de droit interne des parties concernant les preuves électroniques et la cybercriminalité, ainsi que les seuils légaux, les conditions applicables aux preuves et autres qui doivent être remplis pour obtenir la communication de données informatiques stockées en vue de leur utilisation devant les tribunaux.

5.2.4 Les recommandations qui devraient être prises en charge à travers un Protocole additionnel à la Convention de Budapest sur la Cybercriminalité[24]

Rec 19	Les Parties devraient considérer permettre – via des amendements juridiques nationaux et accord international – pour la divulgation rapide de l'identité et l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur.
Rec 20	Les Parties intéressées peuvent considérer la possibilité et le champ d'application d'une injonction de produire internationale qui doit être envoyée directement par les autorités d'une Partie aux agents des services représsifs d'une autre Partie.
Rec 21	Les Parties devraient considérer de renforcer la coopération directe entre autorités judiciaires pour ce qui concerne les demandes d'entraide.
Rec 22	Les Parties devraient pendre en considération la pratique des services répressifs et judiciaires, d'obtenir des données spécifiées relatives au trafic et aux abonnés, directement auprès des fournisseurs de services étrangers, sous réserve de sauvegardes et de conditions.
Rec 23	Les Parties devraient considérer les enquêtes communes et/ou l'établissement d'équipes communes d'enquête entre les Parties.
Rec 24	Les Parties devraient permettre que les demandes soient envoyées en anglais. Les Parties devraient en particulier permettre que les demandes de conservations soient envoyées en anglais.

5.3 Suites à donner

Les Parties sont invitées à donner suite aux recommandations relevant de la responsabilité des autorités nationales et à rendre compte au T-CY dans les 18 mois suivant l'adoption du présent rapport sur les mesures prises, afin de permettre auc règles de procédure (article 2.1.g), d'examiner les progrès accomplis.

Le Secrétariat du Conseil de l'Europe est chargé de donner suite aux recommandations relevant de sa responsabilité et de rendre compte au T-CY dans les 18 mois suivant l'adoption du présent rapport.

Le T-CY doit évaluer la faisabilité d'une suite à donner aux recommandations concernant le « matériel pour le protocole » dans un Protocole additionnel à la Convention sur la cybercriminalité.

[24] Note: Certaines de ces remmandations pourraient également être prises en charge sur le plan national bien que les adressant par le biais d'un Protocole pourrait faciliter eurs reconnaissances par la communauté internationale.

6 Annexes

6.1 Liste des solutions proposées pour prendre l'entraide plus efficiente

Les États ayant répondu au questionnaire ont proposé une large palette de solutions pour rendre l'entraide plus efficiente. Ces solutions sont présentées ici de manière sommaire, et il n'a pas été tenu compte ni de leur faisabilité ni de leur acceptation ou non par les Parties à la Convention sur la cybercriminalité. La plupart de ces solutions sont reflétées dans les « recommandations » du présent rapport.

Proposal 1: Mettre pleinement en œuvre la convention sur la cybercriminalité

1a Mettre pleinement en œuvre la Convention sur la cybercriminalité, y compris en conservant les données stockées.

1b Mettre pleinement en œuvre la Convention sur la cybercriminalité dans le droit des États Parties.

Proposal 2: Ressources – Affecter plus de personnel à l'entraide

2a Affecter davantage de personnel aux questions de cybercriminalité dans les bureaux locaux des procureurs (s'ils exécutent des demandes après que celles-ci aient été reçues).

2b Affecter du personnel plus pointu sur le plan technologique dans les autorités centrales, car les preuves deviendront de plus en plus internationales, et pas l'inverse.

Proposal 3: Meilleure formation

3a Parties : encourager les États à consolider l'entraide, par l'échange de meilleures pratiques et par des activités (conférences, ateliers et autres) ainsi que par l'allocation de ressources. Le Conseil de l'Europe (par le biais de ces programmes de consolidation des capacités) et le T-CY devraient soutenir de telles activités.

3b Autorités centrales ou compétentes pour l'entraide : consolidation des capacités pour les autorités centrales ou compétentes, y compris par la formation, le partage d'expérience et de bonnes pratiques sur l'entraide en matière de cybercriminalité et de preuves électroniques, par l'amélioration des procédures, par le traitement accéléré des demandes et par d'autres activités.

3c Autorités judiciaires : partage de bonnes pratiques, formation et procédures améliorées pour encourager la communication directe entre autorités judiciaires.

3d Juges et Procureurs : formation plus complète et implication des juges et des procureurs dans les questions liées à la cybercriminalité et à la preuve électronique, y compris pour ce qui est de l'utilisation de la Convention de Budapest.

3e Services répressifs : renforcement de la coopération entre services répressifs par des séminaires, des questionnaires, établissement de centres d'excellences nationaux au niveau national et régional (par exemple par le biais des projets de consolidation de capacités du Conseil de l'Europe).

Proposal 4: Meilleure connaissance des critères appliqués par d'autres États

4a Établir un fonds de ressources documentaires en ligne contenant des informations actualisées sur les seuils légaux, les critères en matière de preuve, des lignes directrices pour l'obtention de données et autres critères à remplir pour les demandes d'entraide concernant la communication de données stockées en vue d'une utilisation en justice.

4b Établir une base de données des textes législatifs des parties en matière de preuve électronique et d'infractions pénales connexes.

4c Maintenir un jour des listes de contacts actualisées

Proposal 5: Changements en matière de pouvoirs de la police

5a Permettre, par voie d'amendement législatif, l'obtention directe et plus rapide de renseignements sur des abonnés par un service de police, sans qu'il soit nécessaire d'avoir une injonction de justice.

5b Harmoniser les législations nationales, en permettant à la police et aux autorités judiciaires d'obtenir des données d'identification de base sans commission rogatoire.

5c Donner aux points de contact 24/7 le pouvoir de communiquer partiellement des données stockées, à l'exception des données relatives au contenu.

5d Renforcer les pouvoirs de la police pour l'obtention de données relatives au trafic (sous réserve de mécanismes de co-validation par les autorités judiciaires).

(note : les commentaires du T-CY suggèrent que ces propositions sont complexes et méritent plus amples discussions. La communication de données relatives au trafic peut exiger une décision de justice. L'harmonisation entre toutes les Parties risque d'être difficile à obtenir.)

Proposal 6: Changements dans les régimes légaux

6a Développer un régime d'entraide simplifié et plus rapide entre les Parties à la Convention sur la cybercriminalité.

6b Réexaminer le concept juridique des données relatives au trafic et des informations concernant les abonnés. Pour cela, il sera peut-être nécessaire de procéder à des ajustements de la Directive européenne sur la conservation des données pour ce qui est du type de données couvertes

6c Identifier des solutions pour faciliter l'obtention et la communication accélérées à des autorités étrangères d'informations concernant les abonnés, éventuellement sans entraide ou alors selon une procédure « allégée » (par exemple avec une validation formelle si les données sont utilisées en justice dans un procès pénal). Il conviendra de s'entendre sur les procédures, les critères et les sauvegardes.

6d Permettre aux services répressifs de demander des mandats pour accéder à des communications stockées à la suite d'une demande d'entraide d'un pays étranger.

6e Élaborer, en accord avec les législateurs et les fournisseurs de services sur Internet, un protocole permettant la communication de certains types de données sans demande judiciaire ou commission rogatoire.

6f Permettre aux services répressifs d'obtenir d'un FSI des données stockées relatives au trafic et de les communiquer à services répressifs étrangers sans demande d'entraide formelle (note : il ressort des commentaires que, dans certains pays, la communication de données relatives au trafic ne peut se faire que sur décision d'un tribunal).

6g Permettre aux points de contact 24/7 de traiter directement des demandes d'entraides.

6h Préparer un accord international concernant la juridiction si le siège d'une entreprise se trouve dans un pays, mais que les serveurs sont dans un autre, voire plusieurs autres pays, afin de mieux identifier la cible d'une demande de données (note : il ressort des commentaires que ces règles juridictionnelles sont jugées complexes et difficiles à négocier).

Proposal 7: Utiliser des pouvoirs conservatoires

7a Mettre pleinement en œuvre la convention sur la cybercriminalité, y compris les pouvoirs spécifiques prévus aux articles 16, 17, 29 et 30 en matière de conservation des données[25].

7b Permettre à la police de demander que des communications stockées détenues par un FSI soient conservées au nom d'une autorité répressive étrangère en attendant la réception d'une demande formelle d'entraide.

7c Utiliser davantage les pouvoirs conservatoires afin d'accélérer le processus et de veiller à ce que les données ne sont pas détruites.

7d Garantir à la fois la conservation et la rétention des données.

Proposal 8: Durée de stockage des données par des fournisseurs de services sur Internet

–

8a Les durées de stockage des données prévues par la loi (conservation et rétention) devraient être rendues plus transparentes.

8b Régulation et harmonisation accrues des durées de stockage prévues pour l'ennemi.

8c Harmonisation des durées de conservation des données entre les États.

Proposal 9: Rôle des points de contact 24/7 en matière de demandes d'entraide

9a Les points de contact 24/7 devraient devenir plus proactifs et se faire connaître des autorités de justice pénale pertinentes dans leur pays, ainsi que des autorités étrangères compétentes.

9b Il conviendrait d'organiser des réunions et formations communes du réseau 24/7 pour accroître son efficience.

9c Les points de contact 24/7 devraient jouer au moins un rôle d'appui pour les demandes « article 31 », conformément aux dispositions de l'article 35 de la Convention de Budapest.

9d Des points de contact 24/7 peuvent être établis au sein du parquet pour permettre une plus large gamme d'action et une réponse rapide aux demandes. Transférer, au besoin, des points de contact 24/7 des services répressifs aux services de poursuite, tout en faisant des services répressifs des points de contact secondaires.

9e Les autorités compétentes et points de contact 24/7 devraient envisager des procédures pour suivre, contrôler le traitement et donner un retour d'information à l'État requérant en ce qui concerne des demandes article 31.

9f Les pays peuvent envisager des mécanismes permettant aux points de contact 24/7 de traiter directement les demandes d'entraide, y compris leur exécution.

9g Donner aux points de contact 24/7 le pouvoir d'envoyer ou de recevoir directement des demandes (sans l'intervention du ministère de la Justice avec notification obligatoire du ministère de la Justice ou procureur pertinent).

9h Établir des procédures et une coopération proactive entre les points de contact 24/7 et les autorités compétentes pour l'entraide au niveau des services de poursuite et des ministères de la Justice. Établir des points de contact au niveau de l'autorité centrale (ministère de la Justice), des services de poursuite et de la police.

9i Points de contact 24/7 : organiser des réunions et des formations communes du réseau 24/7 pour en renforcer l'efficience.

9j Points de contact 24/7 : veiller, conformément à l'article 35.3 de la Convention de Budapest, à ce que du personnel formé et équipé soit disponible pour faciliter les travaux opérationnels et mener ou soutenir des activités d'entraide judiciaire.

---

[25] Voir rapport d'évaluation du T-CY sur la conservation : http://www.coe.int/t/dghl/coopération/economiccrime/Source/Cybercrime/TCY/TCY%202013/TCY_2012_10_Assess_report_v30_public.pdf

Proposal 10: Communication directe entre unités chargées de la cybercriminalité ou points de contact 24/7

10a Renforcer la communication directe entre les unités chargées de la cybercriminalité et les points de contact 24/7 des Parties.

Proposal 11: Communication directe entre bureaux des procureurs

11a Des points de contact 24/7 peuvent être établis au sein du parquet pour permettre une plus large gamme d'action et une réponse plus rapide aux demandes d'entraide.

Proposal 12: Communication directe entre autorités centrales et/ou autorités judiciaires

12a Établir des points de contact au niveau de l'autorité centrale (ministère de la Justice), des services de poursuite et de la police pour des demandes article 31 et similaires.

12b Les États devraient utiliser les possibilités de coopération directe entre autorités judiciaires, en particulier du fait que les demandes liées à la cybercriminalité et aux preuves électroniques sont en général considérées comme urgentes. L'article 4 du 2e Protocole additionnelle à la Convention d'entraide pénale ainsi que d'autres accords régionaux et bilatéraux permettent une coopération directe. Ceci réduirait la pression sur les autorités centrales.

Proposal 13: Voies et canaux de communication alternatifs

13a Possible coordination entre les points de contact 24/7 de la Convention de Budapest et ceux d'Interpol, qui se recouvrent partiellement.

13b Utilisation de tous les canaux de coopération internationale disponibles, y compris EUROJUST et le Réseau judiciaire européen.

13c Les canaux d'INTERPOL pourraient être utilisés pour une transmission rapide de demandes d'entraide urgentes.

Proposal 14: Demande de données non liées au contenu directement auprès de fournisseurs de services Internet multinationaux

14a Donner aux services répressifs et de poursuites autorisées le pouvoir de demander directement des données sur le trafic et sur l'abonné aux FSI. Il conviendra de déterminer les critères, sauvegardes et conditions applicables. Ceux-ci peuvent inclure des injonctions de justice nationales.

14b Entrer en contact direct avec des représentants locaux de fournisseurs de services multinationaux.

14c Déterminer le format approprié et les critères à appliquer pour la soumission de demandes directement aux FSI. Dans de nombreux cas, les conditions à remplir se trouvent sur le site Web du FSI concerné.

14d Contacter directement les FSI en cas d'urgence, lorsque cela est toléré ou favorisé par le pays hôte (en particulier les États-Unis).

14e Se rapprocher des FSI dans le contexte de leur politique en vigueur en matière de respect de la loi, qui souvent permettent une coopération directe de ce type avec les autorités étrangères, en particulier si elles ont une représentation légale dans l'Etat requérant.

Proposal 15: Procédures d'urgence

15a Des procédures d'urgence devraient être mises en place pour des demandes lorsqu'il y a risque pour la vie humaine ou dans des circonstances exceptionnelles similaires

Proposal 16: Équipes communes d'enquête

16a Des équipes communes d'enquête devraient être établies pour traiter d'affaires complexes.

16b Il conviendrait d'établir des équipes communes d'enquête entre pays.

Proposal 17: Formulaire type commun pour les demandes d'entraide judiciaire

17a Formulaire type standardisé, plurilingue, pour les demandes « article 31 ». Ceci devrait réduire les frais et les retards induits par la traduction et garantir que les demandes sont complètes et reconnues par les autres Parties.

Proposal 18: Méthodes pour l'envoi de demandes d'entraide

18a Système permettant de faire des catégories ou d'établir des priorités ; les demandes devront être étiquetées selon leur urgence/leur importance afin d'être sûr que les demandes des plus urgentes se voient accorder la priorité la plus élevée.

18b Utiliser davantage les transmissions électroniques afin d'accélérer le processus. Privilégier le courrier électronique, fax, etc. comme moyens et méthodes de communication pour transmettre les demandes - tout en envoyant parallèlement la version originale.

18c Envisager de développer un canal de communication électronique sécurisé pour les demandes d'entraide entre les Parties.

Proposal 19: Procédures d'entraide en général

19a Préparer des procédures opératoires standard pour les demandes d'entraide.

19b Se concerter au préalable au niveau des autorités centrales avant l'envoi formel d'une demande.

19c Utiliser les vidéoconférences dans le contexte de demandes judiciaires étrangères.

19d Encourager les États à renforcer l'entraide et à trouver des solutions pour des affaires difficiles.

Proposal 20: Caractère des demandes

20a Assurer la transparence par les Parties en matière de seuil pour l'exécution de demandes d'entraide. Le caractère véniel d'une infraction ne devrait pas être un motif de refus de la demande. En revanche, le système d'entraide ne devrait pas être engorgé d'affaires vénielles. Les Parties devraient établir des modalités pour le traitement de ce type d'affaires.

20b Formuler des demandes aussi spécifiques et précises que possible. Les demandes trop larges ou trop vagues risquent d'être rejetées.

20c Ne recourir à l'entraide que dans des affaires spécifiques (les faits sont liés au crime organisé ; le préjudice atteint un seuil minimum ; les faits sont d'une gravité exceptionnelle).

20d Donner autant d'informations que possible dans les demandes. Joindre tous les documents et/ou déclarations nécessaires à la demande, ainsi que toute autre information pertinente. Dans le même temps, les Parties doivent trouver des solutions concernant le grand nombre d'informations exigé par l'Etat requérant.

Proposal 21: Langues

21a Lorsqu'il n'est pas possible de disposer rapidement d'une traduction dans la langue nationale de l'Etat requis, pour les commissions rogatoires, il serait bon de privilégier l'anglais.

21b Privilégier l'anglais et le français pour la correspondance.

21c Utiliser des traducteurs plus qualifiés pour une meilleure qualité des traductions des demandes. Éviter d'utiliser des programmes de traduction automatique.

Proposal 22: Réduire les étapes et accélérer le processus

22a Réduire le nombre d'étapes exigées dans le processus d'entraide, notamment en réduisant le nombre d'organisations intermédiaires.

Proposal 23: Délai pour répondre de demandes d'entraide

23a Établir des délais pour répondre aux demandes, ou informer des actions entreprises.

23b Accuser réception des demandes.

Proposal 24: Autres suggestions importantes

24a Établir un forum (en ligne) entre parties prenantes (autorité centrale MJ, procureurs et juges, police, FSI, établissements bancaires, services d'investigations financières et opérateurs de télécommunications)

24b Demander aux FSI de ne pas prévenir les personnes visées par la demande. Les politiques de la plupart des FSI précisent qu'ils informent la personne objet de la demande d'accès qu'ils ont reçu une demande d'accès aux informations la concernant. Si le fait de notifier à la personne concernée qu'une demande d'accès la concernant a été reçue porte atteinte à une enquête criminelle en cours, une injonction judiciaire autorisant la demande d'accès devrait également viser à empêcher le FSI de notifier la réception de cette demande à la personne concernée.

24c Demande directe pour des données stockées de la part de l'autorité judiciaire de l'Etat A – via le point de contact 24/7 – au point de contact 24/7 de l'Etat B pour transmettre la demande au FSI dans l'Etat B avec copie de la demande et résultats aux autorités judiciaires dans l'Etat B afin de contrôler que les conditions sont respectées.

6.2 Compilation de législations nationales pertinentes[26]

6.2.1 Albania

Law no.1093 date 03.12.2009 "On jurisdictional relations with foreign authorities in criminal matters"

Article 7 of the Forwarding a letter request to the competent authority

1. The Ministry of Justice opens the way to a foreign letter request after it evaluates the conditions defined in the domestic legislation.
Subsequently, the letter request is forwarded to the prosecutor of the district where the letter request is to be executed, through the General Prosecutor.

Article 8 Refusal of the letter request

1. The Ministry of Justice and the local judicial authority open the way to a letter request when the conditions defined in the domestic legislation are met.

Article 16 Presence of foreign judicial authorities in the receipt of evidence

1. At the express request of a foreign judicial authority, the local judicial authority gives information about the time and place of execution of the letter rogatory.
2. The court may permit representatives of foreign judicial authorities to take part in the receipt of evidence and to address questions to the person who is questioned according to the rules of the Code of Criminal Procedure.

Article 22 Searching for and sequestration of objects

1. At the request of foreign judicial authorities, a local judicial authority may order the permission of a search of places or the sequestration of items that can be confiscated which are located in the territory of the Republic of Albania in connection with the facts specified in the letter rogatory. The decision may be appealed within 10 days from the day following receipt of knowledge according to the rules of the Coder of Criminal Procedure.
2. The competent local judicial authority performs the search and sequestration in compliance with the rules of the Code of Criminal Procedure.
3. When a third party, who has gained the right in good faith, a state authority or an injured party who has [his] residence or domicile in Albania claims ownership of the objects, documents or profits, the object provided in point 1 of this article are sent only if the foreign judicial authority guarantees their return at the end of the proceedings in connection with the evidence.
4. The sending may be postponed for as long as the objects, documents or profits are necessary for criminal proceedings that have begun in Albania.

Article 23 Delivery of sequestered objects

1. The objects sequestered are send to the foreign judicial authority at its request, in execution of the letter rogatory, to be confiscated or to be returned to the lawful owner.
2. These objects include:
a) objects used for the commission of a criminal offence;
b) objects that come from the commission of a criminal offence or values equivalent to them;

[26] Sur la base des réponses au questionnaire et/ou profils pays.

c) profits from a criminal offence or values equivalent to them;
ç) other objects given with the purpose of inciting the commission of a criminal offence as well as compensation for a criminal offence.
3. The objects or profits may be kept in a permanent manner in Albania if:
a) their owner has [his] residence or domicile in the Republic of Albania;
b) there are serious claims of the Albanian state authorities in connection with the objects or profits;
c) a person, who has not taken part in the commission of a criminal offence and whose claims are not guaranteed by the requesting state proves that he has earned the right to those objects and profits in good faith, as well as that the person has [his] residence in Albania.

Article 24 Postponing the execution of requests

1. A local judicial authority may postpone or condition the execution of requests if it may affect the good conduct of criminal proceedings started by local judicial authorities.
2. The local judicial authority notifies the foreign judicial authority, declaring the reasons for postponement or conditioning. If the notification is made directly to the foreign judicial authority, the local judicial authority informs the Ministry of Justice at the same time.

Article 27 of Law on "On the Jurisdictional Relations with Foreign Authorities in Criminal Matters"

Forwarding data without a request
1. Local judicial authorities even on their own initiative forward to foreign judicial authorities information that is related to criminal offences collected during a criminal proceeding, if they judge that forwarding such information may assist in the opening of a criminal proceeding or the submission of a request for legal assistance from the foreign state. This information is forwarded if the progress of the criminal proceeding in Albania is not hindered and respecting the conditions of reciprocity.
2. The competent local judicial authority may ask the foreign judicial authorities that have received the information mentioned in the first point of this article for data about the measures taken in connection with the information forwarded. In addition, the competent local judicial authority may establish other conditions related to the use of this information in the state to which the information has been forwarded.

Criminal Procedure Code

Article 505 The competencies of the Minister of Justice

1. The Minister of Justice decides to grant support to a letter of application of a foreign authority regarding communications, notifications and the taking of proofs, except when evaluates that the requested actions impair the sovereignty, the security and important interests of the state.
2. The Minister does not grant support to the letter of application when it is certain that the requested actions are prohibited expressly by law or contradict the fundamental principles of the Albanian rule of law. The Minister does not grant support to the letter of application when there are motivated reasons to think that the considerations regarding race, religion, sex, nationality, language, political beliefs or the social state may cause a negative influence to the performance of the process, and when it is certain that the defendant has expressed freely his consent for the letter of application.
3. In cases the letter of application has as subject the summons of the witness, expert or a defendant before a foreign judicial authority, the Minister of Justice does not grant support to the letter of application when the requesting state does not give sufficient guarantee for the non-encroachment of the cited person.
4. The Minister has the right to not grant support to the letter of application in case the requesting state does not give the necessary guarantee of reciprocity.

Article 506 The court proceedings

1. The foreign letter of application cannot be executed unless the court of the place where he must be proceeded has rendered a favourable decision rendered.
2. The district prosecutor, after taking the acts from the Minister of Justice, submits his request to the court.
3. The court disposes of the execution of the letter of application by a decision.
4. The execution of the letter of applications not accepted:
a) in cases the Minister of Justice does not grant support to the letter of application
b) when the fact for which the foreign authority proceeds is not provided as a criminal offence by the Albanian law.

6.2.2 Australia

Mutual Assistance in Criminal Matters Act 1987

Sec. 8 of Mutual Assistance in Criminal Matters Act 1987 of Australia Refusal of assistance

(1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Attorney-General:
(a) the request relates to the prosecution or punishment of a person for an offence that is, or is by reason of the circumstances in which it is alleged to have been committed or was committed, a political offence; or
(b) there are substantial grounds for believing that the request has been made with a view to prosecuting or punishing a person for a political offence; or
(c) there are substantial grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions; or
(d) the request relates to the prosecution or punishment of a person in respect of an act or omission that if it had occurred in Australia, would have constituted an offence under the military law of Australia but not also under the ordinary criminal law of Australia; or
(e) the granting of the request would prejudice the sovereignty, security or national interest of Australia or the essential interests of a State or Territory; or
(f) the request relates to the prosecution of a person for an offence in a case where the person has been acquitted or pardoned by a competent tribunal or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence.
(1A) A request by a foreign country for assistance under this Act must be refused if it relates to the prosecution or punishment of a person charged with, or convicted of, an offence in respect of which the death penalty may be imposed in the foreign country, unless the Attorney-General is of the opinion, having regard to the special circumstances of the case, that the assistance requested should be granted.
(1B) A request by a foreign country for assistance under this Act may be refused if the Attorney-General:
(a) believes that the provision of the assistance may result in the death penalty being imposed on a person; and
(b) after taking into consideration the interests of international criminal co-operation, is of the opinion that in the circumstances of the case the request should not be granted.

(2) A request by a foreign country for assistance under this Act may be refused if, in the opinion of the Attorney-General:
(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would not have constituted an offence against Australian law; or
(b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Australia in similar circumstances would not have constituted an offence against Australian law; or
(c) the request relates to the prosecution or punishment of a person in respect of an act or omission where, if it had occurred in Australia at the same time and had constituted an offence against Australian law, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; or
(d) the provision of the assistance could prejudice an investigation or proceeding in relation to a criminal matter in Australia; or
(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person (whether in or outside Australia); or
(f) the provision of the assistance would impose an excessive burden on the resources of the Commonwealth or of a State or Territory; or
(g) it is appropriate, in all the circumstances of the case, that the assistance requested should not be granted.

Sec.10- Request by Australia

(1) A request for international assistance in a criminal matter that Australia is authorised to make under this Act may be made only by the Attorney-General.

(2) Subsection (1) does not prevent the Attorney-General on behalf of Australia from requesting international assistance in a criminal matter other than assistance of a kind that may be requested under this Act.

Sec.11- Request by foreign country

(1) A request by a foreign country for international assistance in a criminal matter may be made to the Attorney-General or a person authorised by the Attorney-General, in writing, to receive requests by foreign countries under this Act.
(2) A request must be in writing and must include or be accompanied by the following information:
(a) the name of the authority concerned with the criminal matter to which the request relates;
(b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;
(c) a description of the purpose of the request and of the nature of the assistance being sought;
(d) any information that may assist in giving effect to the request.
However, a failure to comply with this subsection is not a ground for refusing the request.
(3) Where a request by a foreign country is made to a person authorised under subsection (1), the request shall be taken, for the purposes of this Act, to have been made to the Attorney-General.
(4) If a foreign country makes a request to a court in Australia for international assistance in a criminal matter:
(a) the court must refer the request to the Attorney-General; and
(b) the request is then taken, for the purposes of this Act, to have been made to the Attorney-General.

15B Requests by foreign countries for stored communications

The Attorney-General may, in his or her discretion, authorise the Australian Federal Police or a police force or police service of a State, in writing, to apply for a stored communications warrant under section 110 of the Telecommunications (Interception and Access) Act 1979 if the Attorney-General is satisfied that:

(a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the **requesting country**) has commenced in the requesting country; and
(b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:
(i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
(ii) a fine of an amount that is at least equivalent to 900 penalty units; and
(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and
(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications.

Telecommunications (Interception and Access) Act 1979

110 Enforcement agencies may apply for stored communications warrants

(1)An enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.
(2)The application must be made on the agency's behalf by:
(a)if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
(b)otherwise:
(i)the chief officer of the agency; or
(ii)an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).
(3)The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.
(4)A nomination under subsection (3) is not a legislative instrument.

116 Issuing of stored communications warrants

(1)An issuing authority to whom an enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:

(a)Division 1 has been complied with in relation to the application; and

(b)in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and

(c)there are reasonable grounds for suspecting that a particular carrier holds stored communications:

(i)that the person has made; or

(ii)that another person has made and for which the person is the intended recipient; and

(d)information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with:

(i)in the case of an application other than a mutual assistance application—the investigation by the agency of a serious contravention in which the person is involved (including as a victim of the serious contravention); or

(ii)in the case of a mutual assistance application—the investigation or investigative proceeding, by the foreign country to which the application relates, of a serious foreign contravention to which the application relates and in which the person is involved (including as a victim of the serious foreign contravention); and

(da)if the stored communications warrant is applied for in relation to a person who is the victim of the serious contravention—the person is unable to consent, or it is impracticable for the person to consent, to those stored communications being accessed; and

(e)in any case—having regard to the matters referred to in subsection (2) or (2A) (as the case requires), and to no other matters, the issuing authority should issue a warrant authorising access to such stored communications.

117 What stored communications warrants authorise

A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:

(a)that was made by the person in respect of whom the warrant was issued; or

(b)that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;

and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

6.2.3 Austria

Article 3 paragraph 2 of the Statute for Police cooperation enables safety authorities in to accomplish mutual assistance

The law enforcement authorities are obliged to render legal assistance also without being requested,

1. by using data that have – owing to their nature – to be transmitted under international law, or
2. if required by a foreign law enforcement authority for the purpose of fulfilling its duties pursuant to s.1, p.1, which states that the International cooperation serves the purposes of the law enforcement (police), CID (Criminal Investigation Division), passport authorities, Aliens Police, and border control on condition of reciprocity,
3. if required for criminal investigation activities by Interpol.

Section 56 para 2 of the Austrian Federal Law on Extradition and Mutual Legal Assistance reads as follows:

"A request for a search of persons or premises, the seizure of objects or monitoring of telecommunications must have attached the original or a certified copy or photocopy of the order from the relevant authority. If not a court order, there must be a statement from the authority seeking the mutual assistance that the conditions required for such measures under applicable law in the requesting country are satisfied."

Extradition and Mutual Assistance Act (ARHG)

Section 3. Reciprocity

(1) A foreign request shall only be complied with provided that it is guaranteed that the requesting State would also comply with a similar request by Austria.

(2) A request may not be filed under this law by an Austrian authority if a similar request by another State were not able to be complied with, except in the event that a request appears to be needed urgently for specific reasons. In this case the requested State shall be notified of the lack of reciprocity.

(3) In the event of doubt over observance of reciprocity, the opinion of the Federal Minister of Justice shall be sought.

(4) Another State may be guaranteed reciprocity in connection with a request made under this law, provided that no intergovernmental agreement exists and that it would be permissible under this law to comply with a similar request of this State.

Direct applicability of the Convention upon its ratification by Austria; see also Section 58 ARHG in connection with Section 143 seq. of the Austrian Code of Criminal Procedure respectively Section 115 of the revised Code of Criminal Procedure (in force from 2008-1-1)

Section 55. Jurisdiction for Processing Letters Rogatory

(1) The district court is competent to process letters rogatory, sections 2 and 3 notwithstanding; in cases where under the 1975 Code of Criminal Procedure, the decision is reserved for the *Ratskammer* or in which there is a request for a search, seizure, temporary injunction or a decision under section 145a of the Code of Criminal Procedure, the court of justice of the first instance in whose district the mutual assistance procedure is to be brought has jurisdiction. Sections 23 and 24 of the 1988 Youth Court Act are applicable as appropriate. If approval of cross-border observation is sought, the court of justice of the first instance in whose district the border will probably be crossed has jurisdiction; in case of observation in an aircraft that flies into Austria,

however, the court of justice in whose district the landing site is located has jurisdiction. Information about a criminal procedure, execution of a prison sentence or preventive measures is issued by the court with jurisdiction; for requests for the transfer of records, the office in which the records are kept has jurisdiction. If a person detained in the prison of a court of justice is to be interrogated, that court of justice has jurisdiction. If the jurisdiction cannot be determined according to these rules, the District Court of the Inner City of Vienna, in cases in which the decision is reserved for the court of justice of the first instance, the Regional Criminal Court of Vienna has jurisdiction.

(2) If a person to be transferred is in prison or preventive custody, the decision on the request for transfer is made by a single judge of the court given in section 16 of the Penal Sentence Enforcement Act, otherwise it is the court on whose order the detention is based. The Federal Ministry of Justice is to be informed of this decision. The Federal Minister of Justice must refuse the transfer if one of the circumstances listed in sections 2 and 3 (1) is present. Transfer at the appropriate border crossing or any other transfer site agreed to be performed by police officers of the Ministry of Justice.

(3) If a person detained in another state is to be transferred through Austria to a third state for important investigative activities, in particular their interrogation or confrontation, sections 44, 47 and 49 apply as appropriate

Direct applicability of the Convention upon its ratification by Austria; to be noted that under Section 3 of the ARHG, mutual assistance can be granted in the absence of a treaty on the basis of reciprocity

Section 58. Applicable Procedures

Mutual assistance is to be provided according to the provisions for criminal procedures within Austria. A request to follow a specific deviating procedure will be granted if this procedure is consistent with the principles of Austrian criminal procedure. If mutual assistance is provided in the form of confiscation (section 143 of the 1975 Code of Criminal Procedure) or a temporary injunction (section 144a of the 1975 Code of Criminal Procedure), this is to be limited in time; the foreign authority making the request is to be informed in the appropriate way.

Section 65

(1) For other criminal offences committed abroad than those referred to in sections 63 and 64 applies the Austrian criminal law, if the offences are also liable to persecution according to the laws which are valid for the scene of the crime:

1. if the offender has been Austrian at the time of the offence or if he has acquired Austrian citizenship at a later date and if he still holds citizenship at the time of initiation of the criminal proceedings;

6.2.4 Bosnia and Herzegovina

Law on Mutual Legal Assistance in Criminal Matters (The Official Gazette of Bosnia and Herzegovina, no. 53/09, 58/13)

Article 3 Letter Rogatory

(1) Request for mutual legal assistance shall be transmitted in the form of Letter Rogatory.
(2) The Letter Rogatory of a foreign judicial authority and the attached documentation must be supported by the translation into one of the official languages of Bosnia and Herzegovina. The translation must be verified by a certified court interpreter.
(3) The Letter Rogatory by a national judicial authority and the attached documentation must be translated into the official language of the requested State.

Article 4 Channels of Communication

(1) Letters Rogatory requesting mutual legal assistance of the national judicial authorities shall be transmitted to foreign judicial authorities through the Ministry of Justice of Bosnia and Herzegovina. Requests for mutual assistance of foreign judicial authorities shall be transmitted to the national judicial authorities through the same channel.
(2) As an exception to Paragraph (1) of this Article, national judicial authorities may directly address the request for mutual legal assistance to a foreign judicial authority, when such a communication is envisaged by an international treaty.
(3) In urgent cases, when such a communication is envisaged by an international treaty, requests for mutual legal assistance may be transmitted and received through the Interpol.
(4) In urgent cases, letters rogatory may be sent and received through Eurojust.
(5) Procedure of competent bodies of Bosnia and Herzegovina in relations with Eurojust, shall be regulated by specific instruction of Miniser of Justice of Bosnia and Herzegovina, by which institutions and contact point for cooperation with Europol will be appointed.
(6) In cases of communication referred to in Paragraphs (2) and (3) of this Article, the national judicial authority shall communicate a copy of the request for mutual legal assistance to the Ministry of Justice of Bosnia and Herzegovina.
(7) The Ministry of Justice of Bosnia and Herzegovina shall transmit and receive through the Ministry of Foreign Affairs of Bosnia and Herzegovina the requests for mutual legal assistance to/from a foreign State that has no international treaty in force with Bosnia and Herzegovina, as well as in cases when an international treaty explicitly envisages use of diplomatic channels of communication.
(8) Requests for mutual legal assistance may also be received if transmitted via electronic or some other means of telecommunication with a written record, and if the foreign relevant judicial authority is willing, upon request, to deliver a written evidence of the manner of transmission and the original request, provided that this manner of transmission is regulated in an international treaty.
Upon receipt of a request from a foreign 24/7 contact point, which contains all the necessary data, the same is delivered to competent BiH police bodies for further proceedings.

Article 5 Urgency of Proceeding

(1) The Ministry of Justice of Bosnia and Herzegovina shall transmit, without delay, request for mutual assistance by a foreign judicial authority to the relevant nationaljudicial authority for further action, unless it is evident that the request is not in compliance with an international treaty and this Law, in which case it should be refused.
"(2) The Ministry of Justice of Bosnia and Herzegovina shall urgently act on the request of national judicial authorities, unless it is obvious that the request does not comply with international treaty and it will be refused by foreign authority. In this case, such a request is returned to the national judicial authority to remedy deficiencies. "

(3) In cases referred to in Article 4 Paragraph (3) of this Law, competent body of Bosnia and Herzegovina for cooperation with Interpol shall communicate the request directly to the relevant national judicial authority, therewith a copy of the request and the sending letter shall submit to the Ministry of Justice of Bosnia and Herzegovina

Article 6 Admissibility and Course of Action

(1) The relevant national judicial authority shall decide on the admissibility and course of action in providing mutual legal assistance requested by a foreign judicial authority in compliance with nationalregulations, unless otherwise stipulated by this Law or an international treaty.
(2) The relevant national judicial authority shall proceed on request by the foreign judicial authority without delay.

Article 7 Forwarding the Letter Rogatory to Relevant Authority

If the authority to which the Letter Rogatory was transmitted is not authorized to proceed, that authority shall forward it without delay to the relevant authority for action, and shall accordingly inform the authority that transmitted the request.

Article 9 Grounds for refusing of legal assistance

(1) Among other reasons prescribed by this law for refusing requests for certain forms of legal assistance, the relevant national judicial authority shall refuse the request for mutual legalassistance:
a) if the execution of the request would prejudice the legal order of Bosnia and Herzegovina or its sovereignty or security;
b) if the request concerns an offense which is considered to be a political offense or an offense connected with a political offense;
c) if the request concerns a military criminal offense.
d) if the person accused of the relevant criminal offense has been acquitted of charges based on the substantive-legal grounds or if the proceeding against him has been discontinued, or if he was relieved of punishment, or if the sanction has been executed or may not be executed under the law of the country where the verdict has been passed;
e) if criminal proceedings are pending against the person in Bosnia and Herzegovina for the same criminal offense, unless the execution of the request might lead to a decision releasing the accused from custody,
f) if criminal prosecution or execution of a sanction pursuant to the national law would be barred by the statute of limitations
(2) The provisions referred to in Paragraph (1) Sub-paragraph d) of this Article shall not apply in cases of reopening the criminal proceedings in the requesting State.
(3) In addition to the reasons stated in paragraph (1) of this Article, legal assistance may be refused on the basis of factual reciprocity in relation to a particular country.

Article 10 Exceptions for refusing of legal assistance

(1) Crimes against humanity or other values protected by international law may not serve as a basis to deny the request for mutual legal assistance in terms of Article 9 Sub-paragraphs b) and c) of this Law.
(2) No request for mutual legal assistance shall be denied solely because it concerns an offense which is considered to be a fiscal offense pursuant to national law.

Article 11 Reasoning the Failure to Execute the Request

The decision refusing the request to afford mutual legal assistance or the failure to execute the request must be reasoned.

Grounds for refusal to cooperate could be an insufficiently elaborated request. Apart from cases referred to in the Convention, the grounds for refusal to cooperate is found in the inability to proceed in cases where there is no criminal offence.

The request, in accordance with the Law on Mutual legal assistance in Criminal Matters (Art. 3, paragraph 2) must be translated into one of the official languages in use in BiH and certified by an authorized court interpreter.

Article 26 (Providing Information without Request)

(1) Without prejudice to their own investigations or proceedings and subject to reciprocity, national judicial authorities may, without a prior request, forward to the relevant foreign judicial authorities information obtained during their own investigations and related to criminal offences if they consider that the disclosure of such information 12 might assist the receiving State in initiating investigations or criminal proceedings or might lead to a request for mutual assistance by that State.

(2) The relevant national judicial authority shall request from the relevant foreign judicial authority to which it transmitted the information referred to in paragraph (1) of this Article communication on any actions undertaken upon such information and it shall also impose other conditions for the use of such information in the receiving State."

Criminal Procedure Code of Bosnia and Herzegovina[27]

Article 72 a Order to the telecommunications operator

(1) If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.
(2) In case of emergency, the Prosecutor may order the measures under Paragraph (1) of this Article, in which case the information received shall be sealed until the issuance of the court order. The Prosecutor shall immediately inform the preliminary proceedings judge, who may issue an order within 72 hours. In case the preliminary proceedings judge does not issue the order, the Prosecutor shall return such information unsealed.
(3) Measures under Paragraph (1) of this Article may also be ordered against a person if there are grounds for suspicion that he will deliver to the perpetrator or will receive from the perpetrator information related to the offence, or grounds for suspicion that the perpetrator uses a telecommunication device belonging to this person.
(4) Telecommunications operators or other legal persons who provide telecommunications services shall enable the Prosecutor and police authorities to enforce the measures referred to in Paragraph (1) of this Article."

[27] The same provision has been prescribed by CPC of Republika Srpska, CPC of Federation of Bosnia and Harcegovina and CPC of Brčko District.

6.2.5 Bulgaria

Section III "A" from MINISTRY OF INTERIOR ACT - „Exchange of Information or Data with the Competent Bodies of the European Union Member States for Prevention, Discovery and Investigation of Crimes (new – SG 93/09, in force from 24.11.2009).

Art. 161a. (new – SG 93/09, in force from 24.11.2009)
(1) Following the provisions of this section the MI through a competent specialized structure shall carry out a simplified exchange of information or data with the competent law enforcement administrations of the European Union Member States, and with the states signatories to the Schengen Agreement for prevention, discovery and investigation of crimes.
(2) The Ministry of Interior through a competent specialized structure may provide:
1. Information and data from the Ministry information funds;
2. Information or data, received from other state bodies or local government authorities, from legal entities and natural persons.
(3) Exchange of information or data with the competent bodies of the European Union Member States and of the states signatories to the Schengen Agreement shall be done subject to observance of th, to which the Republic of Bulgaria is a party, and also subject to observance of the provisions of the Protection of Classified Information Act and the Protection of Personal Data Act.

Art. 161c. (new – SG 93/09, in force from 24.11.2009)
(1) Provision of the required information or data may be withdrawn where there are sufficient grounds to reckon that there is danger of:

1. Establishment of conditions threatening national security and public order;
2. Hindering actions of investigation or gathering data for initiation of penal proceedings;
3. Endangering a natural person's safety.

(2) In addition to the cases under par. 1 provision of required information or data may be refused where they:

1. do not correspond to the objectives, for which they have been requested;

2. are related to a crime, for which the law provides a penalty of imprisonment for a period of up to one year or another less grave penalty.
(3) The requested information or data shall be provided only if permission by the competent judicial body for access to them has been obtained.

Conditions
Art. 161e. (new – SG 93/09, in force from 24.11.2009)
(1) Information or data shall be provided on the grounds of a request by the respective competent body of the Member State.
(2) The request for provision of information or data shall be prepared in one of the official languages of the European Union and shall contain:
1. the justifications, that the respective information of data are available;
2. the purpose for which the information or data are requested;
3. the connection between the purpose and the person, to which the information or data relate.
(3) Information or data, required for prevention, discovery or investigation of crimes under Art. 36 of the Extradition and European Arrest Warrant Act, may be provided without addressing a request.

The Electronic communications act –
Article 251Conditions:

- the request should come from competent authority;
- the grounds that the information or data is available in Bulgaria;
- purpose of the requested data;
- what data exactly is needed (subscriber, traffic, etc.);
- period of time for the data (if applicable – traffic data, etc.);
- data is presented to asking party after a court approval (court order issued for the providers)

EXTRADITON AND EUROPEAN ARREST WARRANT ACT

Conditions for application of the European Arrest Warrant

Art. 36. (*) (1) (amend. – SG 49/10) European Arrest Warrant shall be issued for persons who has committed offences, which carry as per the legislation of the requesting country maximum term of not less than one year imprisonment sentence or a measure requiring detention or another more severe penalty, or if the imposed penalty imprisonment or the requiring detention measure is not shorter than 4 months.

(2) The surrender on the base of European Arrest Warrant shall be performed, if the offence which the warrant has been issued for, constitutes a offence as per the Bulgarian legislation too. Execution of an European Arrest Warrant related to taxes, custom fees or currency exchange cannot be refused on the ground that the Bulgarian legislation does not stipulate the same type of taxes or fees or does not settle the taxes, fees, custom fees or the currency exchange in the same way as the legislation of the issuing Member State does.

(3) (Amend. – SG 49/10) Double criminality shall not be required for the following offences, if in the issuing State they carry maximum term of not less than three years of imprisonment or with another more severe penalty, or for them a measure requiring detention for a maximum term of not less than of 3 years is provided:

1. Participation in a criminal organisation,
2. Terrorism,
3. Trafficking in human beings,
4. Sexual exploitation of children and child pornography,
5. Illicit trafficking in narcotic drugs and psychotropic substances,
6. Illicit trafficking in weapons, munitions and explosives,
7. Corruption,
8. fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests,
9. Laundering of the proceeds of offence,
10. Counterfeiting currency, including of the euro,
11. computer-related offence,
12. Environmental offence, including illicit trafficking in endangered animal species and in endangered plant species and varieties,
13. Facilitation of unauthorised entry and residence,
14. murder, grievous bodily injury,
15. illicit trade in human organs and tissue,
16. kidnapping, illegal restraint and hostage-taking,
17. racism and xenophobia,
18. organised or armed robbery,
19. illicit trafficking in cultural goods, including antiques and works of art,
20. swindling,
21. racketeering and extortion,
22. counterfeiting and piracy of products,
23. forgery of administrative documents and trafficking therein,
24. forgery of means of payment,
25. illicit trafficking in hormonal substances and other growth promoters,
26. illicit trafficking in nuclear or radioactive materials,
27. trafficking in stolen vehicles,
28. rape,
29. arson,
30. offences within the jurisdiction of the International Criminal Court,
31. unlawful seizure of aircraft/ships,
32. sabotage

Criminal Procedure Code

Article 471 Grounds and contents of international legal assistance

(1) International legal assistance in criminal matters shall be rendered to another state under the provisions of an international treaty executed to this effect, to which the Republic of Bulgaria is a party, or based on the principle of reciprocity. International legal assistance in criminal cases shall also be made available to international courts whose jurisdiction has been recognised by the Republic of Bulgaria.

(2) International legal assistance shall comprise the following:

1. Service of process;
2. Acts of investigation;
3. Collection of evidence;
4. Provision of information;
5. Other forms of legal assistance, where they have been provided for in an international agreement to which the Republic of Bulgaria is a party or have been imposed on the basis of reciprocity.

6.2.6 Costa Rica

Article 24 of the Political Constitution of the Republic of Costa Rica:
http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=871&nValor3=88326&strTipM=TC

Law on Registry, Kidnapping and Examination of Private Documents and Intervention of the Communications:
http://www.pgr.go.cr/Scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

Public Ministry's Statutory Law and the Penal Procedural Code:
http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=27760&nValor3=29368&param2=1&strTipM=TC&lResultado=1&strSim=simp

http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=41297&nValor3=91419&param2=2&strTipM=TC&lResultado=12&strSim=simp

6.2.7 Croatia

Act on international legal assistance in criminal matters (Official Gazette 178/04):

Article 4

International legal assistance is afforded in the widest sense in accordance with the principles of domestic order public, the principles of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the International Covenant on Civil and Political Rights.

Article 8

(1) The domestic judicial authority shall act further to the request for international legal assistance of a foreign judicial authority if the request was submitted in written form. The request, and the supporting deeds, have to be accompanied by a translation into the Croatian language, and if that is not possible then into the English language. Translations have to be officially certified.
(2) The domestic judicial authority shall act further to the request for international legal assistance of a foreign judicial authority even if the request was submitted electronically or by some other means of telecommunications leaving a written record, if it may establish its authenticity, and if the competent foreign authority is willing, at request, to deliver a written notice about the method of sending the request and the original request.
(3) Unless an international treaty or this Act provide otherwise, the request for international assistance has to include:
1. The place of issuance and the name of the competent foreign authority sending the request.
2. The legal basis for providing international legal assistance.
3. The exact description of the requested international legal assistance and the reason for the request for international legal assistance.
4. The legal name, a short factual and legal description of the criminal offence (unless the request relates to the service of court decisions, submissions, documents, etc.).
5. Accurate data about and citizenship of the person in relation to whom international legal assistance is sought and his position in the procedure.
6. In the case of service of court deeds, the type of deed being forwarded.

Article 12

(1) The competent domestic authority may refuse the request for international legal assistance if:

1. The request concerns an act regarded as a political criminal offence, an act connected with a political criminal offence,
2. The request concerns a fiscal offence,
3. The execution of the request would likely prejudice the sovereignty, security, ordre public or other essential interests of the Republic of Croatia,
4. It can be justifiably presumed that the person whose extradition is sought would be criminally prosecuted or punished in the case of extradition, because of his race, religion, citizenship, affiliation with a specific social group, or because of his political beliefs, or if his position would be aggravated on the grounds of one of the mentioned reasons,
5. The matter involves an insignificant criminal offence.

(2) Criminal offences or attempted criminal offences against values protected by international law and participation in the commission of such criminal offences cannot be the basis for rejecting a request for international legal assistance within the meaning of paragraph 1, item 1 of this Article.
(3) A request for international legal assistance, because of a fiscal offence from paragraph 1, item 2 of this Act shall not be rejected exclusively because it relates to an act which is a fiscal offence under domestic law.

Article 13

(1) The domestic judicial authority shall reject a request for international legal assistance:

1. If the accused person has been declared not guilty of the same criminal offence in the Republic of Croatia, because of material-legal reasons, or if the procedure against him has been discontinued, or if he has been released from his sentence, or if the sanction has been enforced or cannot be enforced according to the law of the state in which the judgment was adopted,
2. If a criminal proceeding for the same criminal offence is pending in the Republic of Croatia against the accused person, unless the enforcement of the request could lead to a decision on the release of the accused person,
3. If criminal prosecution, enforcement of the sanction or of the security or protective measure would be barred by the statute of limitations under national legislation.

(2) The provisions of paragraph 1, items 1 and 3 of this Article are not applicable in cases where the final judgment was revised in the requesting state.

1) the form of the international legal assistance requested and the reason for the letter rogatory;
2) legal qualification of the criminal offence committed and the summary of the facts, except if the letter rogatory refers to the service of court writs (applications, documents and the like);
3) nationality and other personal details of the person regarding which the international legal assistance is requested and his status in the proceedings;
4) in case of service of court writs, their type.

Article 18

(1) By not interfering with their own investigations or procedures, and under the condition of reciprocity, domestic judicial authorities may send without a prior request to the competent foreign judicial authorities information relating to criminal offences or to infringements of the rule of law from Article 1, paragraph 3 of this Act, gathered in their own investigations, if they believe that the delivery of such information could be of help in the initiation or implementation of an investigation or court procedure or if they could lead to the submission of a request for legal assistance.

(2) The domestic judicial authority shall request from the foreign judicial authority to which it delivered the information from paragraph 1 of this Article notifications about any actions taken further to such information, as well as a copy of all decisions, and it may also impose other conditions for the use of such information in the receiving state.

(3) The information from paragraph 1 of this Article is forwarded through the Ministry of Justice.

6.2.8 Estonia

CPC § 436. Prohibition on international co-operation in criminal procedure

(1) The Republic of Estonia refuses to engage in international co-operation if:
1) it may endanger the security, public order or other essential interests of the Republic of Estonia;
2) it is in conflict with the general principles of Estonian law;
3) there is reason to believe that the assistance is requested for the purpose of bringing charges against or punishing a person on account of his or her race, nationality or religious or political beliefs, or if the situation of the person may deteriorate for any of such reasons.

(1^1) The Republic of Estonia shall not refuse to engage in international co-operation with a Member State of the European Union on the ground that the offence is regarded as a political offence, as an offence connected with a political offence or an offence inspired by political motives unless otherwise provided by law or an international agreement.

CPC § 460. Requirements for requests for assistance

(1) A request for assistance shall set out:
1) the name of the authority making the request;
2) the content of the request;
3) the name, address and, if possible, other contact details of the person with regard to whom the request is submitted;
4) the facts relating to and the legal assessment of the criminal offence concerning which the request is submitted.

CPC § 461. Prohibition on compliance with request for assistance

Compliance with a request for assistance is not permitted and shall be refused on the grounds provided for in § 436 of this Code.

CPC § 462. Proceedings conducted by Ministry of Justice and Public Prosecutor's Office concerning requests for assistance received from foreign states

(1) The Ministry of Justice shall verify whether a request for assistance received from a foreign state meets the requirements. A request in compliance with the requirements shall be immediately sent to the Public Prosecutor's Office.
(2) The Public Prosecutor's Office shall verify whether compliance with the request is admissible and possible and forward the request to the competent judicial authority for execution.
(2^1) In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may complied with the consent of the Public Prosecutor's Office before the request for assistance is received by the Ministry of Justice.
(3) The Ministry of Justice shall forward a request for the service of a summons to the court of first instance of the residence or seat of the person for execution.
(4) If a request for assistance is submitted through Eurojust, Eurojust's National Member for Estonia shall verify whether the request for assistance meets the requirements and whether compliance with the request for assistance is admissible and possible and forward the request to the Estonian competent judicial authority for execution.

CPC § 463. Compliance with requests for assistance received from foreign states

(1) Requests for assistance are complied with pursuant to this Code. At the request of a foreign state, a request may be complied with pursuant to procedural provisions different from the provisions of this Code unless this is contrary to the principles of Estonian law.

(1^1) If summoning of a person to court is required for compliance with a request for assistance, service of the summons shall be organised by the court.
(2) The materials received as a result of compliance with a request shall be sent to the Ministry of Justice through the Public Prosecutor's Office and the Ministry of Justice shall forward the materials to the requesting state.
(3) The materials received as a result of compliance with a request for assistance from a foreign state submitted through Eurojust shall be sent to the requesting state through Eurojust unless otherwise agreed with Eurojust.

6.2.9 Finland

Act on International Legal Assistance in Criminal Matters

Section 8— Language and translations

(1) The request and the accompanying documents shall be in Finnish or in Swedish, or be accompanied by a translation into either of these languages. It may be enacted by Decree that the request and the accompanying documents may be in a foreign language.

(2) A competent authority may execute a request for assistance even where the request and the related documents are in a foreign language provided by Decree or in another foreign language, provided that the execution of the request is not otherwise precluded according to this Act. However, the competent authority may refuse to execute the request, where the request and the documents are not in Finnish or in Swedish, nor accompanied by translations into these languages, if the authority deems that it does not have a sufficient understanding of the language used in the documents. The Ministry of Justice shall be responsible for carrying out translations from foreign languages into Finnish and Swedish as will be enacted by Decree.

(3) A document to be served need not be accompanied by a translation where the service may be executed without a translation under section 17(2).

Section 12— Mandatory grounds for refusal

(1) Assistance shall be refused, where the execution of the request would prejudice the sovereignty, the security or other essential interests of Finland.

(2) Assistance shall be refused, where the execution of the request would be contrary to the principles of human rights and fundamental freedoms or otherwise contrary to Finnish public policy (ordre public).

Section 13— Discretionary grounds for refusal

(1) Assistance may be refused, where:
   (1) the request relates to an offence that is of a political character or an offence under military law only;
   (2) the request relates to an offence, committed by a person who according to Finnish law could no longer be prosecuted by reason of lapse of time, pardon or by any other reason;
   (3) the request relates to an offence which in Finland or in a third State is subject to criminal investigations or under consideration of a prosecution authority or where court proceedings have been initiated;
   (4) the request relates to an offence for which the criminal investigations, prosecution or punishment, or any other punitive sanctions have been waived in Finland or in a third State;
   (5) the request relates to an offence in respect of which the offender has been sentenced or acquitted in Finland or in a third State; or
   (6) the execution of the request would, having regard to the nature of the offence, impose an unreasonable burden on the resources available.

(2) The execution of the request may be postponed, if the execution of the request would cause inconvenience or delay in a criminal investigation, criminal investigations or court proceedings in Finland.

Note:

Regardless of the provisions of general MLA law, assistance will be provided as agreed in international conventions. The Budapest Convention is in force as a law in Finland (similarly as other international conventions to which Finland is a party).

Section 15— Restrictions on coercive measures

(1) Where coercive measures are requested or where the request otherwise involves the use of coercive measures under the Coercive Measures Act (450/1987), such measures shall not be used, where not permitted under Finnish law had the offence to which the request relates been committed in Finland in similar circumstances.

Note: No up to date translation available. However, this legislation states e.g. that paragraph 1 does not apply to preservation order of data referred to in Coercive measures Act.

(2) A suspect or a defendant in criminal proceedings pending in the requesting State who is requested to be examined in Finland in criminal investigations or in court may not be arrested, detained or subjected to a travel ban for the acts or omissions constituting the offence specified in the request.

(3) Where the request relates to the service of a summons to appear before an authority of a foreign State, a Finnish authority may not order the person summoned to obey the summons nor use any measures of compulsion in cases of failure to appear. The duty of witnesses and other persons to obey a summons issued by a court of another Nordic State is governed by the Act on the Duty to Appear Before the Court of Another Nordic Country in Certain Cases (349/1975).

Section 23— Use of coercive measures to obtain evidence or to secure the enforcement of a confiscation order

(1) Search and seizure, telecommunications interception, telecommunications monitoring and technical surveillance in order to obtain evidence as well as identification of persons may be carried out pursuant to a request for assistance made by an authority of a foreign State, if this has been requested or deemed necessary in the execution of the request. (406/1995)

Note: No up to date translation available. However, legislation in force lists also preservation order of data.

(2) Coercive measures may be used upon the request of an authority of a foreign State for the purpose of securing the enforcement in Finland of a confiscation order made or to be made in the requesting foreign State where the order is, or would be, enforceable in Finland.

(3) The use of coercive measures shall be governed by section 15(1) of this Act and by the Coercive Measures Act.

6.2.10 France

Article 695-9-31 à 695-9-47 du Code de procédure Pénale.
http://www.legifrance.gouv.fr/affichCode.do;jsessionid=BD0C632EEFF0AB1BB72863C6DE44A8E9.tpdjo07v_1?idSectionTA=LEGISCTA000024544120&cidTexte=LEGITEXT000006071154&dateTexte=20130411

Art R49-35 à R49-39du Code de procédure pénale
http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=D9318798D21F74DE01CC2DA1848D15D5.tpdjo03v_2?cidTexte=JORFTEXT000025641035&idArticle=LEGIARTI000025642088&dateTexte=20120407

6.2.11 Georgia

Article 10 of the law "On International Law Enforcement Cooperation" a respective law enforcement agency of Georgia will cooperate with a law enforcement agency of a foreign country in the provision and exchange of the following information:

a) Information and data, which will contribute to the prevention, detection and suppression of crimes;
b) Information and personal data related to wanted persons or persons participating in the commission of crime, or persons suspected to participate therein;
c) Information and data related to the offenders' connections, structures of organized groups; typical methods applied by individual offenders and groups, time, place and **modus operandi** of crimes;
d) Information and data related to the acquisition and registration of firearms by a citizen of Georgia in a foreign country or by a citizen of a foreign country in Georgia;
e) Identification data of a motor vehicle and personal data of its owner or user;
f) Criminal intelligence information;
g) Information on the relevant legislation of Georgia;
h) Other information and data determined by bilateral or multilateral treaty or agreement of Georgia, or by the relevant legislation of Georgia.

in article 2 of the law "On International Cooperation in Criminal Matters" that can be formulated as follows:

1. International cooperation in criminal matters is usually carried out on the basis of international treaty of Georgia;
2. In certain cases international cooperation in criminal matters can be also carried out on the basis of reciprocity and individual agreement in case Georgia does not have relevant international treaty with that foreign state;
3. International cooperation based on the principle of reciprocity can be carried out on all issues enshrined in the 1(1) article of this Law despite the extradition and executing judgement of the court;
4. International cooperation based on the principle of reciprocity can be carried out only if reciprocal conditions are clearly formulated and they contain the minimal guarantees provided by this Law without prejudice to establishing higher standards;
5. Individual agreement (ad hoc agreement) can only be concluded for a certain case of mutual assistance and it should contain the minimal guarantees provided by this Law without prejudice to establishing higher standards.

Article 12 (1) of the law "On Cooperation in Criminal Matters" summarised as follows:

2 Georgia will not execute mutual assistance request in case:

a) Executing a mutual assistance request threatens sovereignty, public security or other vital interests of Georgia;
b) Executing a mutual assistance request is not in conformity to the requirements established by Georgian legislation;
c) Crime for which mutual assistance is requested, Georgia considers as politically motivated. Offence shall not be considered as politically motivated in case signs of crime prevail to the alleged political motives;
d) Executing a mutual assistance request endangers human rights and fundamental freedoms;
e) Crime for which mutual assistance was requested is of military character and it is not punishable under the legislation of requesting state unless otherwise provided by the International Treaty of Georgia, Individual Agreement or reciprocal conditions;
f) Executing a mutual assistance request violates the principle **non bis in idem (**Double Jeopardy**)**

Article 12 (2) of the same law provides additional requirements for executing mutual assistance request <u>on search and seizure.</u>

These requirements can be summarised as follows:

a) Mutual assistance can only be carried out if the crime for which mutual assistance was requested, is punishable both under Georgian and respective state's legislation;
b) Mutual assistance can only be carried out if the crime for which mutual assistance was requested is subject to extradition possibility;
c) Mutual assistance can only be carried out if it is otherwise in compliance with Georgian legislation.

6.2.12 Germany

Section 59 IRG Admissibility of Assistance

(1) At the request of a competent authority of a foreign State, other legal assistance in a criminal matter may be provided.
(2) Legal assistance within the meaning of subsection (1) above shall be any kind of support given for foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by an executive authority and whether the legal assistance is to be provided by a court or by an executive authority.
(3) Legal assistance may be provided only in those cases in which German courts and executive authorities could render mutual legal assistance to each other.

Section 66 IRG Handing Over of Objects

(1) At the request of a competent authority of a foreign State objects may be handed over
1. which may serve as evidence in foreign proceedings or
2. which the person concerned or an accomplice have obtained for or through the offence on which the request is based,
3. which the person concerned or an accomplice have obtained through the sale of such object or as a replacement for its being destroyed, damaged or taken away or on the basis of a right accrued to them or as usufruct or
4. which were created by or used or meant to be used in the commission or preparation of the offence on which the request is based.
(2) Surrender shall not be admissible unless
1. the offence on which the request is based contains elements of the actus reus and mens rea of a criminal offence or of an offence permitting the imposition of a fine under German law or unless mutatis mutandis it would be such an offence under German law,
2. an order for seizure by a competent authority of the requesting State is submitted or a declaration of such an authority shows that the requirements for seizure would exist if the objects were located in the requesting State and
3. measures are in place to ensure that the rights of third parties will not be infringed and that objects handed over under a condition will be returned upon request without undue delay.
(3) The handing over under subsection (1) nos. 2 to 4 above shall be admissible only as long as no pertinent final and enforceable foreign decision exists with regard to the abovementioned objects.
(4) The public prosecution service at the Landgericht shall prepare the decision about the handing over and shall execute it if granted. The public prosecution service at the Landgericht in whose district the object is located shall have jurisdiction. S. 61(2) 2nd sentence shall apply mutatis mutandis.

Section 94 CCP [Objects Which May Be Seized]

(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95 CCP [Obligation to Surrender]

(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 96 CCP [Official Documents]

Submission or surrender of files or other documents officially impounded by authorities or public officials may not be requested if their highest superior authority declares that publication of the content of these files or documents would be detrimental to the welfare of the Federation or of a German *Land*. The first sentence shall apply *mutatis mutandis* to files and other documents held in the custody of a Member of the Federal Parliament or of a *Land* parliament or of an employee of a Federal or *Land* parliamentary group where the agency responsible for authorizing testimony has made a corresponding declaration.

Section 97 CCP [Objects Not Subject to Seizure]

(1) The following objects shall not be subject to seizure:
1. written correspondence between the accused and the persons who, according to Section 52 or Section 53 subsection (1), first sentence, numbers 1 to 3b, may refuse to testify;
2. notes made by the persons specified in Section 53 subsection (1), first sentence, numbers 1 to 3b, concerning confidential information entrusted to them by the accused or concerning other circumstances covered by the right of refusal to testify;
3. other objects, including the findings of medical examinations, which are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 1 to 3b, to refuse to testify.
(2) These restrictions shall apply only if these objects are in the custody of a person entitled to refuse to testify unless the object concerned is an electronic health card as defined in section 291a of Part Five of the Social Code. Objects covered by the right of physicians, dentists, psychological psychotherapists, psychotherapists specializing in the treatment of children and juveniles, pharmacists and midwives to refuse to testify shall not be subject to seizure either if they are in the custody of a hospital or a service provider which collects, processes or uses personal data for the persons listed, nor shall objects to which the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 3a and 3b, to refuse to testify extends, be subject to seizure if they are in the custody of the counselling agency referred to in that provision. The restrictions on seizure shall not apply if certain facts substantiate the suspicion that the person entitled to refuse to testify participated in the criminal offence, or in accessoryship after the fact, obstruction of justice or handling stolen goods, or where the objects concerned have been obtained by means of a criminal offence or have been used or are intended for use in perpetrating a criminal offence, or where they emanate from a criminal offence.
(3) Insofar as the assistants (Section 53a) of the persons mentioned in Section 53a subsection (1), first sentence, numbers 1 to 3b, have a right to refuse to testify, subsections (1) and (2) shall apply *mutatis mutandis*.
(4) The seizure of objects shall be inadmissible insofar as they are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, number 4, to refuse to testify. This protection from seizure shall also extend to objects which the persons mentioned in Section 53 subsection (1), first sentence, number 4, have entrusted to their assistants (Section 53a). The first sentence shall apply *mutatis mutandis* insofar as the assistants (Section 53a) of the persons mentioned in Section 53 subsection (1), first sentence, number 4, have a right to refuse to testify.
(5) The seizure of documents, sound, image and data media, illustrations and other images in the custody of persons referred to in Section 53 subsection (1), first sentence, number 5, or of the editorial office, the publishing house, the printing works or the broadcasting company, shall be inadmissible insofar as they are covered by the right of such persons to refuse to testify. Subsection (2), third sentence, and Section 160a subsection (4), second sentence, shall apply *mutatis mutandis*; in these cases, too, seizure shall only be admissible, however, where it is not disproportionate to the importance of the case having regard to the basic rights arising out of Article 5 paragraph (1), second sentence, of the Basic Law, and the investigation of the factual circumstances or the establishment of the whereabouts of the perpetrator would otherwise offer no prospect of success or be much more difficult.

Section 98 CCP [Order of Seizure]

(1) Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a court order shall apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a court decision. The competence of the court shall be determined by Section 162. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.
(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within three days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The agency making the request shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 98a CCP [Automated Comparison and Transmission of Personal Data]

(1) Notwithstanding Sections 94, 110 and 161, where there are sufficient factual indications to show that a criminal offence of substantial significance has been committed
1. relating to the illegal trade in narcotics or weapons or the counterfeiting of money or official stamps,
2. relating to national security (sections 74a, 120 of the Courts Constitution Act),
3. relating to offences which pose a danger to the general public,
4. relating to endangerment of life and limb, sexual self-determination or personal liberty,
5. on a commercial or habitual basis, or
6. by a member of a gang or in some other organized way,

personal data relating to individuals who manifest certain significant features which may be presumed to apply to the perpetrator may be automatically matched against other data in order to exclude individuals who are not under suspicion or to identify individuals who manifest other significant characteristics relevant to the investigations. This measure may be ordered only where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult.
(2) For the purposes of subsection (1), the storing agency shall extract from the database the data required for matching purposes and transmit it to the criminal prosecuting authorities.
(3) Insofar as isolating the data for transmission from other data requires disproportionate effort, the other data shall, upon order, also be transmitted. Their use shall not be admissible.
(4) Upon request by the public prosecution office, the storing agency shall assist the agency effecting the comparison.
(5) Section 95 subsection (2) shall apply *mutatis mutandis*.

Section 98b CCP [Competence; Return and Deletion of Data]

(1) Matching and transmission of data may be ordered only by the court and, in exigent circumstances, also by the public prosecution office. Where the public prosecution office has made the order, it shall request court confirmation without delay. The order shall become ineffective if it is not confirmed by the court within three working days. The order shall be made in writing. It shall name the person obliged to transmit the data and shall be limited to the data and comparison characteristics required for the particular case. The transmission of data may not be ordered where special rules on use, being provisions under Federal law or under the

corresponding *Land* law, present an obstacle to their use. Sections 96 and 97, and Section 98 subsection (1), second sentence, shall apply *mutatis mutandis*.
(2) Regulatory and coercive measures (Section 95 subsection (2)) may be ordered only by the court and, in exigent circumstances, also by the public prosecution office; the imposition of detention shall be reserved to the court.
(3) Where data was transmitted on data media these shall be returned without delay once matching has been completed. Personal data transferred to other data media shall be deleted without delay once it is no longer required for the criminal proceedings.
(4) Upon completion of a measure pursuant to Section 98a, the agency responsible for monitoring compliance with data protection rules by public bodies shall be notified.

Section 98c CCP [Comparison of Data to Clear Up a Criminal Offence]

In order to clear up a criminal offence or to determine the whereabouts of a person sought in connection with criminal proceedings, personal data from criminal proceedings may be automatically matched with other data stored for the purposes of criminal prosecution or execution of sentence, or in order to avert danger. Special rules on use presenting an obstacle thereto, being provisions under Federal law or under the corresponding *Land* law, shall remain unaffected.

Section 99 CCP [Seizure of Postal Items]

Seizure of postal items and telegrams addressed to the accused which are held in the custody of persons or enterprises providing, or collaborating in the provision of, postal or telecommunications services on a commercial basis shall be admissible. Seizure of postal items and telegrams shall also be admissible where known facts support the conclusion that they originate from the accused or are intended for him and that their content is of relevance to the investigation.

Section 100 CCP [Jurisdiction]

(1) Only the court and, in exigent circumstances the public prosecution office, shall be authorized to implement seizure (Section 99).
(2) A seizure ordered by the public prosecution office, even if it has not yet resulted in a delivery, shall become ineffective if it is not confirmed by the court within three working days.
(3) The court shall have the authority to open the delivered post. The court may transfer this authority to the public prosecution office insofar as this is necessary so as not to endanger the success of the investigation by delay. The transfer shall not be contestable; it may be revoked at any time. So long as no order has been made pursuant to the second sentence, the public prosecution office shall immediately forward the delivered postal items to the court, leaving any unopened postal items sealed.
(4) The court competent pursuant to Section 98 shall decide on a seizure ordered by the public prosecution office. The court which ordered or confirmed the seizure shall decide whether to open an item that has been delivered.
(5) Postal items in respect of which no order to open them has been made are to be forwarded to the intended recipient without delay. The same shall apply insofar as there is no necessity to retain the postal items once opened.
(6) Such part of a retained postal item as does not appear expedient to withhold for the purposes of the investigation is to be transmitted to the intended recipient in the form of a copy.

6.2.13 Italy

C.P.P

Art. 696. Prevalenza delle convenzioni e del diritto internazionale generale.

1. Le estradizioni, le rogatorie internazionali, gli effetti delle sentenze penali straniere, l'esecuzione all'estero delle sentenze penali italiane e gli altri rapporti con le autorità straniere, relativi all'amministrazione della giustizia in materia penale, sono disciplinati dalle norme della Convenzione europea di assistenza giudiziaria in materia firmata a Strasburgo il 20 aprile 1959 e dalle altre norme delle convenzioni internazionali in vigore per lo Stato e dalle norme di diritto internazionale generale.
2. Se tali norme mancano o non dispongono diversamente, si applicano le norme che seguono.

Art. 723. Poteri del ministro di grazia e giustizia.

1. Il ministro di grazia e giustizia dispone che si dia corso alla rogatoria di un'autorità straniera per comunicazioni, notificazioni e per attività di acquisizione probatoria, salvo che ritenga che gli atti richiesti compromettano la sovranità, la sicurezza o altri interessi essenziali dello Stato.
2. Il ministro non dà corso alla rogatoria quando risulta evidente che gli atti richiesti sono espressamente vietati dalla legge o sono contrari ai principi fondamentali dell'ordinamento giuridico italiano. Il ministro non dà altresì corso alla rogatoria quando vi sono fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire negativamente sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla rogatoria.
3. Nei casi in cui la rogatoria ha ad oggetto la citazione di un testimone, di un perito o di un imputato davanti all'autorità giudiziaria straniera, il ministro di grazia e giustizia non dà corso alla rogatoria quando lo Stato richiedente non offre idonea garanzia in ordine all'immunità della persona citata.
4. Il ministro ha inoltre facoltà di non dare corso alla rogatoria quando lo Stato richiedente non dia idonee garanzie di reciprocità.

6.2.14 Japan

Act on International Assistance in Investigation and Other Related Matters

Article 8 (1) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may take the following measures:

(i) To ask any person concerned to appear and interview the person;
(ii) To request an expert opinion;
(iii) To carry out an inspection;
(iv) To request the submission of a document or other material to its owner, possessor or custodian;
(v) To request a public office, or a public or private organization to report on necessary matters;
(vi) To request in writing, a person who engages in the business of providing electronic communication facility for communications of others or a person whose facility for his own electronic communications is capable of transmitting electronic communications among many or unspecified persons to preserve necessary part of the electromagnetic records, which are recorded in the course of business, by specifying the origin, destination, time and other traffic data of the electronic communication for a period not exceeding 30 days (if to extend, not exceeding 60 days in total).

(2) With regard to the collection of evidence necessary for assistance, a public officer or a judicial police officer may, if deemed necessary, undertake seizure, seizure of data medium recorded under an order, search, or inspection of evidence, upon a warrant issued by a judge.

Law n°89 of 2004

Article 3

1. A request for assistance shall be received, and evidence shall be forwarded to the requesting country, by the Minister of Foreign Affairs. The Minister of Justice, however, may carry out these tasks, upon a consent given by the Minister of Foreign Affairs, when a treaty confers the authority to receive requests for assistance on the Minister of Justice, or where exigency or other special circumstances exist.

2. When the Minister of Justice receives a request for assistance or forwards evidence to the requesting country in accordance with the second sentence of the preceding paragraph, the Minister of Justice may ask the Minister of Foreign Affairs for cooperation necessary for the execution of matters relating to the assistance.

Law n°89 of 2004

Article 2

Assistance shall not be provided in any of the following circumstances:
(1) When the offense for which assistance is requested is a political offense, or when the request for assistance is deemed to have been made with a view to investigating a political offense;

(2) Unless otherwise provided by a treaty, when the act constituting the offense for which assistance is requested would not constitute an offense under the laws, regulations or ordinances of Japan were it committed in Japan;

(3) With respect to a request for an examination of a witness or a submission of material evidence, unless otherwise provided by a treaty, when the requesting country does not clearly demonstrate in writing that the evidence is indispensable to the investigation.

Article 4

Upon receiving a request for assistance, the Minister of Foreign Affairs shall, except where any of the following applies, forward the written request for assistance or a certification prepared by the Minister of Foreign Affairs of the fact that such a request has been made , as well as related documents, with the opinion of the Minister of Foreign Affairs attached, to the Minister of Justice:

(1) When a request has been made based on a treaty, where the form of the request does not satisfy the reqirements of the treaty;

(2) When a request has been made without being based on a treaty, where there is no guarantee from the requesting country that it will honor requests of the same sort from Japan.

Article 15

When the Minister of Justice, after taking measures as provided for in paragraph l, item (2) or (3) of Article 5, or in paragraph 2 of Article 5, deems it to be inappropriate to provide assistance, he/she shall, without delay, notify the person who has received the documents concerning the request for assistance to that effect.

6.2.15 Latvia

Criminal procedure law

Article 845. - Grounds for the Assistance to a Foreign State in the Performance of Procedural actions

The following are grounds for procedural assistance:
1) a request of a foreign state regarding the provision of assistance in the performance of a procedural action;
2) a decision of a competent authority of Latvia regarding the admissibility of a procedural action.

6.2.16 Lithuania

Article 6 Paragraph 3 of the Law on Police Activities of the Republic of Lithuania

"The police may provide data, in the manner prescribed by legislation of the European Union, international treaties and other legal acts of the Republic of Lithuania, to law enforcement agencies of foreign states as well as to international law enforcement organisations for the purposes of detection, investigation and prevention of criminal acts, ensuring of public order, rendering of emergency assistance to persons when it is necessary because of their physical or mental helplessness, as well as to persons who have suffered from criminal acts, other violations of law, natural calamities or similar acts." (Law No. XI-444, 22 October 2009, entered into force since 31 October 2009, Official Gazette, No. 130-5637, 2009).

Criminal Code of the RL

Article 119. Espionage

1. A person who, for the purpose of communicating it to a foreign state or organisation thereof, seizes, purchases or otherwise collects the information constituting a state secret of the Republic of Lithuania or communicates this information to a foreign state, organisation thereof or their representative
shall be punished by imprisonment for a term of two up to ten years.
2. A person who, in performing an assignment of another state or organisation thereof, seizes, purchases or otherwise collects or communicates the information constituting a state secret of the Republic of Lithuania or another information of interest to the intelligence of a foreign state
shall be punished by imprisonment for a term of three up to fifteen years.

Article 124. Unlawful Possession of the Information Constituting a State Secret

A person who unlawfully acquires or conveys the information constituting a state secret of the Republic of Lithuania or unlawfully holds in possession the material items whose content or information thereon constitutes a state secret of the Republic of Lithuania, in the absence of characteristics of espionage,
shall be punished by a fine or by arrest or by imprisonment for a term of up to three years.

Article 125. Disclosure of a State Secret

1. A person who discloses the information constituting a state secret of the Republic of Lithuania, where this information was entrusted to him or he gained access thereto through his service, work or in the course of performance of public functions, but in the absence of characteristics of espionage,
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by imprisonment for a term of up to three years.
2. The act provided for in paragraph 1 of this Article shall be a crime also where it has been committed through negligence.

Article 166. Violation of Inviolability of a Person's Correspondence

1. A person who unlawfully intercepts a postal item or package sent by post or via a provider of courier services or unlawfully intercepts, records or observes a person's messages transmitted by electronic communications networks or unlawfully records, wiretaps or observes a person's conversations transmitted by electronic communications networks or otherwise violates inviolability of a person's correspondence
shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two year.
2. A legal entity shall also be held liable for an act provided for in this Article.

Article 167. Unlawful Collection of Information about a Person's Private Life

1. A person who unlawfully collects information about a person's private life shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to three years.
2. A legal entity shall also be held liable for an act provided for in this Article.

Article 168. Unauthorised Disclosure or Use of Information about a Person's Private Life

1. A person who, without another person's consent, makes public, uses for his own benefit or for the benefit of another person information about the private life of another person, where he gains access to that information through his service or profession or in the course of performance of a temporary assignment or he collects it through the commission of an act provided for in Articles 165-167 of this Code,
shall be punished by community service or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to three years.
2. A legal entity shall also be held liable for an act provided for in this Article.
3. A person shall be held liable for an act provided for in this Article only subject to a complaint filed by the victim or a statement by his authorised representative or at the prosecutor's request.

Article 210. Commercial Espionage

A person who unlawfully acquires the information considered to be a commercial secret or communicates this information to another person
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

Article 211. Disclosure of a Commercial Secret

A person who discloses the information considered to be a commercial secret which was entrusted to him or which he accessed through his service or work, where this act incurs major property damage to the victim,
shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by a fine or by restriction of liberty or by arrest or by imprisonment for a term of up to two years.

Article 296. Seizure or Other Unlawful Acquisition of an Official Secret

A person who seizes, purchases or otherwise unlawfully acquires a material item whose content or information thereon constitutes an official secret or transfers the item or information thus acquired to a third party, in the absence of characteristics of espionage or provision of assistance to a foreign state, shall be punished by a fine or by arrest or by imprisonment for a term of up to two years.

Article 297. Disclosure of an Official Secret

1. A person who discloses the information constituting an official secret which was entrusted to him or which he accessed through his service or work, in the absence of characteristics of espionage or assistance to a foreign state in carrying out activities hostile to the Republic of Lithuania, shall be considered to have committed a misdemeanour and shall be punished by deprivation of the right to be employed in a certain position or to engage in a certain type of activities or by a fine or by restriction of liberty.
2. The act provided for in this Article shall be considered as criminal also where it has been committed through negligence."

6.2.17 Moldova

Criminal Procedure Code of the Republic of Moldova

Article 531. Legal regulation of international legal assistance

(1) Relations with foreign countries or international courts on legal assistance in criminal matters are covered in this chapter and the provisions of the Law on International Legal Assistance in Criminal Matters. Provisions of international treaties to which Moldova is a party and other international obligations of the Republic of Moldova will have precedence over the provisions of this chapter.

(2) If the Republic of Moldova is party to several international legal instruments to which the State is a party to legal assistance is requested or the requesting State and divergences arise between the rules of such acts or inconsistencies, the provisions of the treaty that provides beneficial protection of human rights and freedoms.

(3) Ministry of Justice can decide to not execute a court decision on the admission of international legal assistance in case of the fundamental national interests are disputable. This task is exercised fully to respect the rights of litigants in the execution of judgments in their favor.

Article 534. Refusal to international legal assistance

(1) International legal assistance may be refused if:

1) the request relates to offenses considered in the Republic of Moldova as political offenses or offenses connected with such crimes. Refusal is not admissible if the person is suspected, accused or sentenced for the committing of offenses under article 5-8 from the Rome Statute of the International Criminal Court;
2) the request concerns an offense which is solely a violation of military discipline;
3) the requested for legal assistance criminal prosecution body or court consider that execution likely to prejudice the sovereignty, security or public policy of the state;
4) there are reasonable grounds to believe that the suspect is criminally prosecuted or punished on account of race, religion, nationality, association with a particular group or political beliefs, shared, or if his situation will further aggravate for listed grounds;
5) it is proved that the person in requesting state will not have access to a fair trial;
6) the respective offense is punishable with death under the law of the requesting State and the requesting State gives no warranty for non-application or non-performance penalty;
7) under the Criminal Code of the Republic of Moldova, the invoked in the request offense or offenses are not an offense;
8) in accordance with national law, a person can not be held to criminal liability.

(2) Any refusal on international legal assistance will be motivated.

Article 536. Addressing the letter rogatory

(1) The criminal prosecution body or the court, if considered necessary making a procedural action in a foreign state, letters rogatory addressed by the criminal investigation body or the court of that State or an international criminal court under international treaty to which Moldova is a party or by diplomatic means, in terms of reciprocity.

(2) Conditions of reciprocity is confirmed in a letter that the Minister of Justice and General Prosecutor undertakes to grant, on behalf of the Republic of Moldova, legal assistance to foreign state or to international criminal court conducting procedural actions, guaranteeing procedural rights provided by national law of the person against whom assistance is made.

(3) Rogatory commission in the Republic of Moldova shall be submitted by the prosecution to the General Prosecutor and by the court - Minister of Justice submission for execution to the respectove state.

(4) A demand of rogatory commission and attached documents shall be drawn up in the official language and are translated into the language of requested State or in another language, according to provisions or reserves to applicable international treaty.

Article 537

(1) The request for the rogatory commission shall be done in writing and must include:

1) name of the body that addresses with the request;

2) name and address, if known, of the institution to which the request is sent;

3) international treaty or reciprocal agreement under which assistance is requested;

4) indicate criminal case in which is requested legal assistance, information about facts that have committed their actions and the legal text article of the Criminal Code of the Republic of Moldova and data on the damage caused by the offense;

5) data on persons who requested the rogatory commission, including their procedural capacity, date and place of birth, citizenship, residence, occupation, for legal entities - their name and address and the name and addresses of their representatives people when necessary;

6) the claim and data necessary to carry them with exposure circumstances which will be found, the list of documents, material evidence and other evidence requested, the circumstances on which the test is to be administered and the questions that need to be made to persons to be heard.

7) the date which is expected to reply to the request and, where appropriate, a request to allow the execution respective procedural actions to assist the criminal investigation body representative of the Republic of Moldova.

(1^1) at the rogatory commission request is attached the procedural acts necessary to carry out criminal actions, prepared in accordance with the provisions of this Code.

(2) The request for rogatory commission and the attached documents are signed and authenticated by the official stamp of the competent institution demanding.

Article 538.

Validity procedural act Procedural document issued in a foreign country in accordance with the law of that country applies to the prosecuting authorities and the courts of the Republic of Moldova.

Article 539. Quoting witnesses, experts or people being pursued over outside the Republic of Moldova

(1) A witness, expert or prosecuted person, if that is not search time, are outside Moldova may be called by the prosecution to perform certain procedural actions in Moldova. In this case, the summons can not contain injunction forced to bring into the law enforcement body.

(2) summoning the witness or expert shall be as provided in art.536 par. (3) and (4).

(3) actions with the participation of persons summoned under this Article shall be made under this Code.

(4) A witness, expert or prosecuted person, regardless of their nationality, who appeared before the body that has requested following a summons under this Article shall not be prosecuted or detained or subjected to any other restriction of freedom their individual Moldovan territory for acts or convictions anterior border of the Republic of Moldova.

(5) The immunity provided in par. (4) ceases if the person cited has not left the territory of the Republic of Moldova within 15 days of the date on which organ called her/his and informed him that his presence is no longer required and then returned to Moldova. In this term does not include the time the person cited could not leave Moldova for reasons beyond his control.

(6) Citation detainee in a foreign state shall be made under this Article, provided that the person temporarily transferred in Moldova by the respective authority of the foreign country to perform the actions

specified in the request for transfer will be returned within the time stated in request. Conditions of transfer or refusal of transfer is regulated by international treaties to which the Republic of Moldova and the requested country are part of or pursuant to obligations under the mutual written.

(7) A witness or expert quoted is entitled to demand reimbursement of expenses for travel, accommodation and subsistence expenses incurred in connection with absence from work reasons.

(8) The witness heard under this article shall, as appropriate, beneficiate of protection under the law.

Article 540[1]. Search, collection, remittance objects or documents, seizure and confiscation

Rogatory commission requesting a search, increasing or remission of objects or documents, as well as seizure or confiscation are executed in accordance with the legislation of the Republic of Moldova.

Article 540. Execution in Moldova of the rogatory commission required by foreign authorities

(1) The criminal prosecution body or the court executed the requested rogatory commission by foreign bodies such under international treaties to which the Republic of Moldova and the applicant are partially or reciprocal confirmed according to art.536 par. (2).

(2) The request for rogatory commission shall be sent by the General Prosecutor Office to the criminal investigation body or, where appropriate, by the Ministry of Justice to the court of the place where they are to be carried procedural action required.

(4) At the execution of the rogatory commission, the provisions of this code, however, at the request of the requesting Party may apply a special procedure under the law of the foreign country in accordance with international treaty itself or on condition of reciprocity, unless it conflicts with national and international obligations of the Republic of Moldova.

(5) At the execution of the rogatory commission, can assist representatives from foreign state or international court if it is stipulated by an international treaty or a question written on a reciprocal obligation. In this case, at the request of the applicant, the body entrusted with the execution of the rogatory commission informs the requesting Party of the time, place and time of execution of the rogatory commission in order that interested parties can attend.

(6) If the person against whom enforcement is sought is indicated wrong rogatory commission, the body entrusted with the execution of the measures in order to determine the address. If address setting is not possible, notify the applicant about it.

(7) In case if the rogatory commission request may not be executed, documents received shall be returned to the requesting Party through the institutions from which they received, and the reasons that prevented execution. Request of rogatory commission and attached documents shall be returned and in case of refusal on the grounds provided in art.534.

Article540[2]. Joint investigation teams

(1) The competent authorities of two or more states may constitute agreement, a joint investigation team for a specific purpose and for a limited period may be extended by mutual consent, to conduct a criminal investigation or in several of the states that constitute the team. Joint investigation team composition is decided by mutual agreement.

(2) Joint investigation teams can be created when:

1) In a prosecution pending in the requesting State should be carried out difficult prosecutions involving mobilization of substantial resources regarding other states;

2) More States are conducting criminal investigations that require coordinated, concerted action in those countries.

(3) Demand for training joint investigation team may be made by any state involved. Joint investigation team is formed in one of the States to be made criminal.

(4) Demand for training joint investigation team comprising authority which made the request, subject and reason for the request, the identity and nationality of the person, name and address, if applicable, and its proposals for the composition.

(5) Components joint investigation team appointed by Moldovan authorities as members, while members appointed by a foreign state are members posted.

(6) Joint investigation team's work in Moldova is carried out according to the following rules:

1) Joint investigation team leader is a representative of the authority participating in criminal proceedings in the Member State in whose territory the team and act within its powers under its national;

2) the team shall carry out the law of the Republic of Moldova. Team members and seconded members perform their tasks under the responsibility of the person referred to in section 1), taking into account the conditions set by their own authorities in the agreement on team building.

(7) Seconded members beside joint investigation teams are entitled to attend any procedural, unless the team leader, for special reasons decides otherwise.

(8) When joint investigation team is to perform procedural acts in that State, seconded members may request their own competent authorities to take those measures.

(9) A member of the next joint investigation team may, under its national law and its powers are to provide information to the team that posted the state in the purpose of the prosecution.

(10) Information lawfully obtained by a member or seconded member while part of a joint investigation team that can not be obtained otherwise by the competent authorities of the states concerned may be used:

1) the purpose for which it was created team;
2) for discovering, investigating and prosecuting other criminal offenses with the consent of the state in which the information was obtained;
3) for preventing an immediate and serious threat to public security, respecting the provisions of section 2);
4) other purposes, if it is agreed by states formed team.

(11) In case of joint investigation teams operating in the republic of Moldova, seconded members of the team are treated as members of the Republic of Moldova regarding crimes committed against them or by them.

6.2.18 Montenegro

Law on International Legal Assistance in Criminal Matters

Article 3

International legal assistance shall include extradition of the accused and sentenced persons, transfer and assuming of criminal prosecution, enforcement of foreign criminal verdicts, delivery of documents, writs and other cases associated with the criminal proceedings in the requesting state, as well as the undertaking of certain procedural actions such as: hearing of the accused, witnesses and experts, crime scene investigation, search of premises and persons and temporary seizure of items.

Article 4

The Ministry responsible for the judiciary (hereinafter referred to as the Ministry) shall be a central communication authority through which domestic judicial authorities shall forward letters rogatory for international legal assistance to foreign judicial authorities and vice versa.
In cases when this has been provided for under an international agreement or where there is reciprocity, the Ministry shall submit letters rogatory to the central communication authority of the requested state, and in cases where there is no such agreement or reciprocity, the Ministry shall deliver and receive letters rogatory for international legal assistance through diplomatic channels.
Without prejudice to the above, if provided for under an international agreement, domestic judicial authorities may deliver letters rogatory for international legal assistance to a foreign judicial authority directly and they shall be obliged to deliver the copy of the letter rogatory to the Ministry.
In urgent cases, provided that there is reciprocity, letter rogatory for international legal assistance may be delivered through the National Central Bureau – INTERPOL.
The higher court and the state prosecutor shall be responsible for provision of international legal assistance in accordance with the law.

Article 5

The Ministry shall deliver, without delay, the letters rogatory from foreign judicial authorities to domestic judicial authorities, except in cases when it is obvious that the letter rogatory should be rejected.
The permissibility and the method of enforcement of the action which is the subject matter of a foreign judicial authority shall be decided by the court in accordance with domestic legislation and ratified international agreements.

Article 6

The basis for provision of international criminal assistance shall be that the offence for which the provision of international legal assistance is requested is a criminal offence both under the domestic law and under the law of the requesting country the judicial authority of which presented the letter rogatory

Article 7

Unless otherwise has been provided for by an international agreement or this Law, signed and certified letter rogatory for international legal assistance shall contain:

1) the name and the seat of the authority making the request;
2) the name of the requested authority, and if its precise name is unknown, an indication that the letter rogatory is being sent to the competent judicial authority, and the name of the country;
3) legal basis for the provision of international legal assistance;

4) the form of the international legal assistance requested and the reason for the letter rogatory;
5) legal qualification of the criminal offence committed and the summary of the facts, except if the letter rogatory refers to the service of court writs (applications, documents and the like);
6) nationality and other personal details of the person regarding which the international legal assistance is requested and his status in the proceedings;
7) in case of service of court writs, their type.

6.2.19 Netherlands

Articles 552h to 552s and Articles 552jj to 552vv of the Dutch Code of Criminal Procedure (DCCP) shall be taken into account.

Article 552(h) DCCP provides that the title relates to the requests for mutual legal assistance that have been made in connection with a criminal case. So, there have to be foreign criminal proceedings in the investigation, prosecution, handling in court and execution phase. The crimes committed must be punishable according to the law of the requesting state. Since a coercive measure has to be applied in the territory of the Netherlands, i.e. obtaining stored data, the act should be punishable under Dutch law. Furthermore, this criminal offence should be listed in Article 67 DCCP, which sums up offences for which pre-trial detention is allowed.
Extract Criminal Procedure Code:
http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html#3857, select "Titel X. Internationale Rechtshulp"

6.2.20 Norway

Norwegian Criminal Procedure Act does not have specific regulation of cooperation with law enforcement in other jurisdictions. Article 215a (expedited preservation of data) does refer to request from other countries as a possible background for expedited preservation.

Norwegian Courts of Justice Act, Article 46, first subsection, Norwegian courts can only process a request from courts or authorities in other countries if the request is sent through the relevant Norwegian Ministry (The Ministry of Justice), unless otherwise is stated.

6.2.21 Portugal

Cybercrime Law - Law nr 109/2009

Article 20 - International cooperation

The national authorities shall cooperate with the competent foreign authorities for the purpose of criminal investigations or proceedings relating computer systems or data, as well as the collection of evidence of a crime in electronic form, according to the rules on transfer of personal data contained in Law No 67/98 of 26 October.

Article 22 - Preservation and expedited disclosure of computer data within international cooperation

1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data.
2 - The request specifies:
a) the authority requesting the preservation;
b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto;
c) the computer data to be retained and its relation to the offense;
d) all the available information to identify the person responsible for the data or the location of the computer system;
e) the necessity of the measure of preservation, and
f) The intention to submit a request for assistance for search, seizure and disclosure of the data.
3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them.
4 - Preservation can also be ordered by *Polícia Judiciária*, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article.
5 - A preservation order specifies, on penalty of nullity:
a) the nature of the data;
b) if known, the source and their destination, and
c) the period of time during which that data must be preserved for up to three months.
6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity.
7 - The competent judicial authority, or *Policia Judiciária* with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year.
8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request.
9 - Data preserved under this Article may only be provided:
a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17;
b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13.
10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data.
11 – The provisions of paragraphs 1 and 2 shall apply, *mutatis mutandis*, to requests sent to other authorities by the Portuguese authorities.

Article 23 - Grounds for refusal

1 - A request for expedited preservation or disclosure of computer data is refused if:
a) the computer data in question refer to a political offense or a related offense according to Portuguese law;
b) it attempts against the sovereignty, security, *ordre publique* or other constitutionally defined interests of the Portuguese Republic;
c) the requesting State does not provide guarantees for the protection of personal data.
2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.

Article 24 - Access to computer data within international cooperation

1 – In the execution of the request of the foreign authority, the competent judicial authority may proceed with the search, seizure and disclosure of data stored in the computer system located in Portugal, related to crimes defined in Article 11, when the search and seizure would be admissible in a similar national case.
2 - The judicial authority shall proceed as quickly as possible when there is reason to believe that the computer data in question are particularly vulnerable to loss or modification, or where cooperation is provided for an expedited instrument of cooperation described in any international legal instrument.
3 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.

Article 25 - Cross-border access to computer data stored when publicly available or with consent
The competent foreign authorities without prior request from the Portuguese authorities, in accordance with the rules on transfer of personal data provided by Law No. 67/98 of 26 October, may:
a) access data stored in a computer system located in Portugal, where publicly available;
b) receive or access through a computer system located in its territory, the data stored in Portugal, through legal and voluntary consent of the person legally authorized to disclose them.

Article 26 - Interception of communications within international cooperation
1 - Pursuant to a request by the competent foreign authority it may be authorized by the judge the interception of computer data transmissions from a computer system located in Portugal, since it is stipulated by a treaty or an international agreement and whether it is a case where such interception is allowed under Article 18, in a similar national case.
2 – *Policia Judiciária* is the responsible entity for receiving requests to intercept communications, which report to the Public Prosecution Service, so as they can be presented to the judge in charge of the *comarca* of Lisbon for authorization.
3 - The referred order of authorization also allows the immediate transmission of the communication to the requesting State, if such a procedure is foreseen in a treaty or an international agreement under which the request is made.
4 - The provisions of paragraph 1 shall apply, *mutatis mutandis*, to requests made by Portuguese judicial authorities.

Article 145-A of the general framework of the judicial cooperation (Law Nr 144/99, of 31 August, as amended by Laws Nr 104/2001, of 25 August, Law Nr 48/2003, of 22 August, Law Nr 48/2007 of 29 August and Law Nr 115/2009 of 12 October - Law on International Judicial Co-operation in Criminal Matters)

6.2.22 Romania

L302/2004 (Article 11 - Direct transmission)

(1) Requests for international judicial assistance in criminal maaters may be sent directly by the requesting judicial authorities to the requested judicial authorities if the international judicial instrument applicable in the relation between the Requesting State and the Requested State regulates this type of transmission.
(2) With the exception of the case mentioned in para.(1), requests for international judicial assistance can be sent directly by the requesting judicial authorities to the requested judicial authorities in case of emergency; however, a copy of these shall be sent simultaneously to the Ministry of Justice or to the Public Prosecutor's Office attached to the High Court of Cassation and Justice, according to case.
(3) The procedure mentioned in para.(1) and (2) shall be used also for transmitting replies to emergency requests for judicial assistance.
(4) In the case under para. (1) and (2), direct transmissions can be made through the International Criminal Police Organisation (Interpol).

ARTICLE 12 - Other modalities of sending the requests

(1) In order to send requests, based on the agreement between the Requesting and the Requested States, adequate electronic means may be used as well, in particular fax, when available, if the authenticity and confidentiality of the request, as well as the credibility of the data sent are guaranteed.
(2) The previous paragraph shall not prevent the use of the emergency means provided in Article 11.

- Law no. 302/2004 on International Judicial Cooperation in Criminal Matters (republished)
- Law No. 161/2003 Title III (The Prevention and Countering of Cyber-Crime)
- Law no. 508/ 2004 on the Creation, Organization and Operation of the Directorate for Investigating Organized Crime and Terrorism
- Law 39/2003 on the Prevention and Combating of Organized Crime
- Law 656/2002 on the Prevention and Sanctioning of Money Laundering

Article 8 (Non bis in idem) of the Law no 302/2004 provides that international judicial cooperation is not admissible when, in Romania or in any other State, criminal prosecution has taken place for the same act and if:
a) a final jugement stated the acquittal or ceasing of the criminal trial;
b) the penalty imposed through a final sentence has been served or was subject to a pardon or amnesty, either as a whole or a the part of it;
(2) Paragraph (1) shall not apply if assistance is requested in order to review the final decision, for one of the reasons that justify the promotion of a means of extraordinary judicial appeal provided in the Romanian Criminal Procedure Code.
(3) Paragraph (1) shall not apply where an international treaty to which Romania is part of contains conditions that are more favourable as regards the principle of non bis in idem.

6.2.23 Serbia

Law on Mutual Assistance In Criminal Matters of Republic of Serbia

Article 7

1) The criminal offence, in respect of which legal assistance is requested, constitutes the offence under the legislation of the Republic of Serbia;
2) The proceedings on the same offence have not been fully completed before the national court, that is, a criminal sanction has not been fully executed;
3) The criminal prosecution, that is, the execution of a criminal sanction is not excluded due to the state of limitations, amnesty or an ordinary pardon;
4) The request for legal assistance does not refer to a political offence or an offence relating to a political offence, that is, a criminal offence comprising solely violation of military duties;
5) The execution of requests for mutual assistance would not infringe sovereignty, security, public order or other interests of essential significance for the Republic of Serbia.

List of the grounds for refusal of request for MLA according **to Law on Mutual Assistance in Criminal Matters**:

1) the criminal offence, in respect of which legal assistance is requested, doesn`t constitute the offence under the legislation of the Republic of Serbia;
2) the proceedings on the same offence have been fully completed before the national court, that is, a criminal sanction has been fully executed;
3) the criminal prosecution, that is, the execution of a criminal sanction is excluded due to the state of limitations, amnesty or an ordinary pardon;
4) the request for legal assistance refer to a political offence or an offence relating to a political offence, that is, a criminal offence comprising solely violation of military duties;
5) the execution of requests for mutual assistance would infringe sovereignty, security, public order or other interests of essential significance for the Republic of Serbia.

6.2.24 Slovakia

Code of Criminal Procedure	Trestný priadok
Letters Rogatory of Foreign Authorities	**Dožiadania cudzích orgánov**
Section 537 **Method and Form of Letters Rogatory Processing**	**§ 537** **Spôsob a forma vybavenia dožiadania**
(1) The Slovak authorities shall perform the legal assistance requested by the foreign authorities in the manner regulated by this Act or an international treaty. If legal assistance is provided under an international treaty in a manner which is not governed by this Act, the competent public prosecutor shall decide in what manner the legal assistance should be performed.	(1) Slovenské orgány vykonávajú právnu pomoc požadovanú cudzími orgánmi spôsobom upraveným v tomto zákone alebo v medzinárodnej zmluve. Ak sa poskytuje právna pomoc podľa medzinárodnej zmluvy postupom, ktorý nie je upravený v tomto zákone, rozhodne príslušný prokurátor, akým spôsobom sa právna pomoc vykoná.
(2) The requested legal assistance may be performed upon the request of a foreign authority under a legal regulation of the requesting State, if the requested procedure is not contrary to the interests protected by the provisions of Section 481.	(2) Na žiadosť cudzieho orgánu možno požadovanú právnu pomoc vykonať podľa právneho predpisu dožadujúceho štátu, ak žiadaný postup nie je v rozpore so záujmami chránenými ustanovením § 481.
(3) For the performance of letters rogatory under Section 539 Subsection 1, it is requested that the act, which the letters rogatory concern, is a criminal offence not only under the legal system of the requesting State, but also the legal system of the Slovak Republic.	(3) Na vykonanie dožiadania podľa § 539 ods. 1 sa vyžaduje, aby čin, ktorého sa dožiadanie týka, bol trestným činom nielen podľa právneho poriadku dožadujúceho štátu, ale aj právneho poriadku Slovenskej republiky.
Section 538 **Jurisdiction for the Processing of Letters Rogatory**	§ 538 **Príslušnosť na vybavenie dožiadania**
(1) The letters rogatory of a foreign authority for legal assistance shall be served to the Ministry of Justice.	(1) Dožiadania cudzieho orgánu o právnu pomoc sa zasielajú ministerstvu spravodlivosti.
(2) To ensure the processing of a letter rogatory from a foreign authority for legal assistance, the district prosecution, under which jurisdiction the requested act of legal assistance is to be performed, is competent. If the local jurisdiction is given to several public prosecutions, the Ministry of Justice shall send the letters rogatory to the Attorney General's Office for a decision as to which of the public prosecutions shall provide its processing.	(2) Na zabezpečenie vybavenia dožiadania cudzieho orgánu o právnu pomoc je príslušná okresná prokuratúra, v ktorej obvode sa požadovaný úkon právnej pomoci má vykonať. Ak je daná miestna príslušnosť viacerých prokuratúr, zašle ministerstvo spravodlivosti dožiadanie generálnej prokuratúre na rozhodnutie, ktorá prokuratúra zabezpečí jeho vybavenie.
(3) If a foreign authority requests the performance of an interrogation or another act of legal assistance by the court due to the application of the act in the criminal proceedings in the requesting State, the public prosecutor shall submit the letters rogatory of a foreign authority to this extent to the District Court under which jurisdiction the act of legal assistance is to be performed, for processing. If the subject of the letters rogatory is solely an act which is to be performed by the court, the Ministry of Justice shall serve the request directly to the competent court.	(3) Ak cudzí orgán požiada o vykonanie výsluchu alebo iného úkonu právnej pomoci súdom z dôvodu použiteľnosti úkonu v trestnom konaní v dožadujúcom štáte, predloží prokurátor v tejto časti dožiadanie cudzieho orgánu na vybavenie okresnému súdu, v ktorého obvode sa úkon právnej pomoci má vykonať. Ak predmetom dožiadania je výlučne úkon, ktorý má vykonať súd, zašle ministerstvo spravodlivosti dožiadanie priamo príslušnému súdu.
Section 539 **Permission of an Act of Legal Assistance for the Courts**	**§ 539** **Povolenie úkonu právnej pomoci súdom**
(1) If the order of the court under this Act is necessary for the performance of evidence requested by a foreign authority, the court shall issue an order upon the petition of the public prosecutor providing the processing of the letters rogatory.	(1) Ak sa podľa tohto zákona vyžaduje na vykonanie dôkazu požadovaného cudzím orgánom príkaz súdu, vydá príkaz súd na návrh prokurátora zabezpečujúceho vybavenie dožiadania.
(2) If the act of legal assistance is to be performed under a foreign regulation, the court shall decide, upon the petition of the public prosecutor, whether the procedure under the foreign regulation is not contrary to the interests protected by the provisions of Section 481. If they do not find such conflict, the act shall be permitted and they shall simultaneously decide on the manner of its performance. The public prosecutor may file a complaint against the decision of the court, which has a suspensive effect. The decision of the court on the conflict of the procedure under a	(2) Ak sa úkon právnej pomoci má vykonať podľa cudzieho predpisu, rozhodne súd na návrh prokurátora, či postup podľa cudzieho predpisu nie je v rozpore so záujmami chránenými ustanovením § 481. Ak takýto rozpor nezistí, úkon povolí a súčasne rozhodne, akým spôsobom sa vykoná. Proti rozhodnutiu súdu môže prokurátor podať sťažnosť, ktorá má odkladný účinok. Rozhodnutie súdu o rozpore postupu podľa cudzieho predpisu sa nevyžaduje, ak ide o doručenie písomnosti alebo poučenie osoby podľa

foreign regulation shall not be required if it is a serving of documents or instruction of the person under a foreign regulation. (3) The District Court under which jurisdiction the act of legal assistance is to be performed is competent to make a decision under Subsection 1 and 2.	cudzieho predpisu. (3) Na rozhodnutie podľa odsekov 1 a 2 je príslušný okresný súd, v ktorého obvode sa úkon právnej pomoci má vykonať.

Section 90 of the Code of Criminal Procedure **Preservation and Disclosure of Computer Data**	**§ 90 Trestného poriadku** **Uchovanie a vydanie počítačových údajov**
(1) If the preservation of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including traffic data that is stored through a computer system, the presiding judge and, before the initiation of the criminal prosecution or in the preliminary hearing, the public prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to	(1) Ak je na objasnenie skutočností závažných pre trestné konanie nevyhnutné uchovanie uložených počítačových údajov vrátane prevádzkových údajov, ktoré boli uložené prostredníctvom počítačového systému, môže predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor vydať príkaz, ktorý musí byť odôvodnený aj skutkovými okolnosťami, osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, aby
a) store such data and maintain the integrity thereof,	a) také údaje uchovali a udržiavali v celistvosti,
b) allow the production or retention of a copy of such data,	b) umožnili vyhotovenie a ponechanie si kópie takých údajov,
c) render access to such data impossible,	c) znemožnili prístup k takým údajom,
d) remove such data from the computer system,	d) také údaje odstránili z počítačového systému,
e) release such data for the purposes of the criminal proceedings.	e) také údaje vydali na účely trestného konania.
(2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data storage shall be performed must be determined. This period may be up to 90 days, and if its re-storage is necessary, a new order must be issued.	(2) V príkaze podľa odseku 1 musí byť ustanovený čas, po ktorý bude uchovávanie údajov vykonávané, tento čas môže byť až na 90 dní, a ak je potrebné ich opätovné uchovanie, musí byť vydaný nový príkaz.
(3) If the storage of the computer data, including the traffic data for the purpose of the criminal proceedings, is no longer necessary, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, shall issue an order for the revocation of the storage of such data without undue delay.	(3) Ak uchovávanie počítačových údajov vrátane prevádzkových údajov na účely trestného konania už nie je potrebné, vydá predseda senátu a pred začatím trestného stíhania alebo v prípravnom konaní prokurátor bez meškania príkaz na zrušenie uchovávania týchto údajov.
(4) The order under Subsection 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order.	(4) Príkaz podľa odsekov 1 až 3 sa doručí osobe, v ktorej držbe alebo pod jej kontrolou sa nachádzajú také údaje, alebo poskytovateľovi takých služieb, ktorým sa môže uložiť povinnosť zachovať v tajnosti opatrenia uvedené v príkaze.
(5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1.	(5) Osoba, v ktorej držbe alebo pod jej kontrolou sa nachádzajú počítačové údaje, vydá tieto údaje, alebo poskytovateľ služieb vydá informácie týkajúce sa týchto služieb, ktoré sú v jeho držbe alebo pod jeho kontrolou, tomu, kto vydal príkaz podľa odseku 1.
Section 115 of the Code of Criminal Procedure	**§ 115 Trestného poriadku**
(8) If the interception and recording of telecommunication operations did not find any facts relevant to the criminal proceedings, the law enforcement authority or the competent department of the Police Force must destroy such recordings in the prescribed manner without undue delay. A transcript on the destruction of the recordings shall be entered into the file. The authority, by whose decision the matter was finally concluded and, in proceedings before the court, the presiding judge of the court of first instance, shall notify the	(8) Ak sa pri odpočúvaní a zázname telekomunikačnej prevádzky nezistili skutočnosti významné pre trestné konanie, orgán činný v trestnom konaní alebo príslušný útvar Policajného zboru musí získaný záznam predpísaným spôsobom bez meškania zničiť. Zápisnica o zničení záznamu sa založí do spisu. O zničení záznamu osobu uvedenú v odseku 3, ktorá nemá možnosť nazerať do spisu podľa tohto zákona, upovedomí orgán, ktorého rozhodnutím sa vec právoplatne skončila, a v konaní pred súdom predseda

person referred to in Subsection 3, who does not have the possibility of inspecting the file under this Act, on the destruction of the recordings within three years after the final termination of the criminal prosecution in the given matter; this shall not apply if it is performed on a particularly serious crime or a crime committed by an organised group, criminal group or a terrorist group, or if several persons participated in the commission of the criminal offence and, in relation to at least one of them, the criminal prosecution was not finally concluded, or if the provision of such information could obstruct the purpose of the criminal proceedings.	senátu súdu prvého stupňa do troch rokov od právoplatného skončenia trestného stíhania v danej veci; to neplatí, ak sa koná o obzvlášť závažnom zločine alebo zločine spáchanom organizovanou skupinou, zločineckou skupinou alebo teroristickou skupinou, alebo ak sa na trestnom čine podieľalo viac osôb a vo vzťahu aspoň k jednému z nich nebolo trestné stíhanie právoplatne skončené, alebo ak by poskytnutím takej informácie mohol byť zmarený účel trestného konania.
(9) The provisions of subsection 1 through 8 shall apply accordingly to content data or traffic data that is transmitted through a computer system in real time.	(9) Ustanovenia odsekov 1 až 8 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje, ktoré sú v reálnom čase prenášané prostredníctvom počítačového systému.
Section 116 of the Code of Criminal Procedure	**§ 116 Trestného poriadku**
(1) In criminal proceedings for an intentional criminal offence, an order for the determination and notification of data on the performed telecommunications operation, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued.	(1) V trestnom konaní pre úmyselný trestný čin možno vydať príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke, ktoré sú predmetom telekomunikačného tajomstva alebo na ktoré sa vzťahuje ochrana osobných údajov, ktoré sú potrebné na objasnenie skutočností dôležitých pre trestné konanie.
(2) The warrant for the establishment and notification of data on the performed telecommunication operations shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing upon the petition of the public prosecutor, the judge for preliminary hearing, in writing which must be justified by its merits; the warrant shall be served to the persons referred to in Subsection 3.	(2) Príkaz na zistenie a oznámenie údajov o uskutočnenej telekomunikačnej prevádzke vydáva písomne predseda senátu, pred začatím trestného stíhania alebo v prípravnom konaní sudca pre prípravné konanie na návrh prokurátora, ktorý musí byť odôvodnený aj skutkovými okolnosťami; príkaz sa doručí osobám uvedeným v odseku 3.
(3) The legal entities or natural persons that provide the telecommunication operations must notify the presiding judge and, in the preliminary hearing, the public prosecutor or police officer, about the data on the performed telecommunication operations.	(3) Právnické osoby alebo fyzické osoby, ktoré zabezpečujú telekomunikačnú prevádzku, oznámia predsedovi senátu a v prípravnom konaní prokurátorovi alebo policajtovi údaje o uskutočnenej telekomunikačnej prevádzke.
(4) The provisions of subsection 1 through 3 shall apply accordingly to content data or traffic data transmitted through a computer system.	(4) Ustanovenia odsekov 1 až 3 sa primerane vzťahujú na obsahové údaje alebo prevádzkové údaje prenášané prostredníctvom počítačového systému.

6.2.25 Slovenia

Provisions from Criminal Procedure Code

148th Article

(1) If there are grounds for suspicion that a crime was committed for which the offender is prosecuted ex officio, the police must take steps necessary to trace the offender, that the offender or participant does not hide or flee, to detect and protect the traces of a criminal offense and objects which may be used as evidence and to collect all information that could be useful for the successful conduct of criminal proceedings.

Article 149b

(1)If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the state prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an adducement of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator of the electronic

Article 164

(1) The police may even prior to the initiation seize items at 220th of this Act, if it would be dangerous to delay, and the conditions of the 218th of this Act to make home and personal investigation.

220th Article (seizure of items)

(1) Items which must be take under criminal or may be evidence in criminal proceedings shall be seized and deposited with the court or otherwise protect their storage.

(2) A person who has such items must delivered them at the request of the court. If he does not deliver the items, they can to be punished by a fine specified in the first paragraph of Article 78 of this Act, if he still don't want to do, he can be put in prison. Prison lasts until the surrender of items or until the end of criminal proceedings, but more than one month.

(4) Police officers may seize items mentioned in the first paragraph of this Article, when act in connection with 148 and 164 Article of this Act or when they issuing the court order.

Article 515

(3) If reciprocity or if so stipulated by an international treaty, international criminal-law also provides direct assistance to local and international bodies involved in the pre-trial and criminal proceedings. It may use modern technical means, in particular computer network devices for transmission of images, voice and electronic impulses.

6.2.26 Switzerland

Les bases juridiques régissant l'entraide judiciaire en matière pénale sont la *Loi sur l'entraide internationale en matière pénale* (EIMP), l'ordonnance y relative (OIEMP) et la *Convention européenne d'entraide judiciaire en matière pénale* (CEEJ). Ces textes règlent les principes généraux de l'entraide et la rendent subsidiaire à un cadre formel plus au moins strict. Citons par exemple l'art. 16 al. 2 CEEJ qui statue que les Parties peuvent décider dans quelle langue les demandes d'entraide doivent lui être adressées et que le principe de réciprocité est applicable. Etant donné que l'art. 28 al. 5 EIMP prévoit que les demandes d'entraide vers la Suisse doivent être rédigées en une langue nationale, les autres Etats peuvent exiger de même pour les demandes de la Suisse. Cela signifie que pour les demandes d'entraide envers les Etats dont la langue n'est pas maîtrisée par la Suisse, un service de traduction est indispensable.

Federal Act on International Mutual Assistance in Criminal Matters (Mutual Assistance Act, IMAC):
http://www.admin.ch/ch/e/rs/351_1/index.html

6.2.27 "The former Yugoslav Republic of Macedonia"

Chapter XXX of CPC, (Article 502-508)

Article 502
PROCEDURE FOR APPROVAL OF INTERNATIONAL JUDICIAL ASSISTANCE AND EXECUTION OF INTERNATIONAL TREATIES IN JUDICIAL CRIMINAL CASES

The international judicial criminal assistance will be performed according to the provisions of this law in line with the provisions of the European Convention for the international judicial assistance in the criminal matter with the Protocols, European Convection of United Nations for trans national organize crime and with other international treaties ratified in accordance with the Constitution of Republic of Macedonia

Article 503

(1) The applications of the domestic courts for judicial assistance in the criminal cases are delivered to the foreign agencies in a diplomatic course. In the same manner to the domestic courts are delivered the applications of the foreign agencies for judicial assistance, through the Ministry of Justice or directly from the competent court".(2) In emergencies, if there is mutuality, the applications for judicial assistance may be delivered by the Ministry of internal affairs.
(2) By law it will be determined which courts will be competent for giving international judicial criminal assistance and one court may be assigned to perform the work for all the courts on a certain region.

Article 504

(1) The Ministry of External Affairs will direct the application of the foreign agency for judicial assistance to the Ministry of Justice which will direct it for a procedure to the court on which region the person resides, who has to be handed a writ or who has to be examined or confronted or on which region another investigating act has to be conducted.
(2) In cases under Article 503, paragraph 2 of this Code, the Ministry of Internal Affairs directs the application to the court by the Ministry of Justice.
(3) On the permission and manner of the conducting of the act, which is the case in the application of the foreign agency, decides the court according to the domestic regulations.
(4) When the application refers to a crime for which according to the domestic regulations extradition is not allowed, the court will request an instruction from the Ministry of Justice.

Article 505

(1) The domestic courts may accept the application of the foreign agency with which it is requested execution of the criminal sentence by the foreign court or on the international court"
if it is determined with an international treaty, or if there is reciprocity or if the sanction is also pronounced by the domestic court according to the Criminal Code.
(2) The competent court reaches the verdict at the Chamber under Article 22, paragraph 6 of this Code. The public prosecutor and the counsel will be informed of the session of the Chamber.
(3) The local competence of the court is determined according to the last residence of the convicted person in the Republic of Macedonia- according to his place of birth. If the convicted person has not a residence nor was born in the Republic of Macedonia, the Supreme Court of the Republic of Macedonia will determine one of the courts to be competent before which the procedure will be conducted.
(4) The competent court is the court which is determined by law.
(5) In the pronouncement of the verdict under paragraph 2 of this Article, the court will insert the complete pronouncement and the title of the court with the foreign verdict and will pronounce a sanction, appropriate with the verdict pronounced by the foreign court". In the elaboration of the verdict will be presented the reasons for which the court has pronounced the sanction.

(6) Against the verdict may appeal the public prosecutor and the convicted person or his counsel.
(7) If the foreign citizen convicted by a domestic court or if the person authorised with an agreement submits an application to the first degree court the convicted person to serve the sentence in his country, the first degree court will act according to the international treaty
(8) Execution of the verdicts brought by the international court has to be performed in accordance with international treaties ratified in accordance with the Constitution of Republic of Macedonia.
(9) The Criminal Council from article 22 (6) of this law , on the local-govern first degree court, with verdict is confirming the authenticity and execution of the international court verdict and determines the manner of the sanction or the other measures of execution.

Article 505 –a

Domestic courts are proceeding upon the application of the foreign organs for overtaking the temporary measures for ensuring the article 203-a from this law, or towards the execution of measure for property confiscation and property interest and seizure of the objects towards which they have proceeded in accordance with the provisions from the international agreement.
The confiscated property and the property interest or the seized objects could be renounced with the court decision from the foreign country under certain conditions defined with the international agreement.
The domestic (national) courts under special defined conditions which are determined with the international contract can request determination of the temporary measures for ensuring that article 203- a of this law and execution of the confiscation of property and the property interest and seizing of the objects from the foreign organs
In the case when with the international agreement it is regulated that the confiscated property and the property interest shall be divided between the Republic of Macedonia and some other state, such of proposal will be delivered by the Ministry for justice. to the foreign country.

Article 506

For the crimes- making and releasing counterfeit bank notes, unauthorised production and trade with the narcotic drugs, psychotropic substances and precursors, trafficking with human beings, enterprising of pornographic material on child"
as well as other crimes in view of which with the international treaties it is determined centralisation of data, the court before which the criminal procedure is conducted, without delay, is obliged to deliver to the Ministry of Internal Affairs the data for the crime, the criminal and the legally valid verdict.

Article 507

(1) If on the territory of the Republic of Macedonia a crime has been committed by a foreigner who has a residence in a foreign country, out of the circumstances under Article 510 of this Code, to that country may be transferred all criminal records for the criminal prosecution and trial, if the foreign country is not against it.
(2) Before the decision for investigation is brought, the decision for transferring is brought by the competent public prosecutor. During the investigation, the decision on the proposal of the public prosecutor is brought by the investigating judge, and by the beginning of the trial, the Chamber (Article 22, paragraph 6).
(3) Transferring may be allowed for crimes for which a sentence to ten years is anticipated, as well as for the crimes- endangering the public traffic.
(4) If the damaged is a citizen of the Republic of Macedonia, transferring is not allowed if he resists it, unless it is allowed security for realisation of his lawful property request.
(5) If the accused is detained, from the foreign country it will be requested in the briefest possible way within 40 days to state whether it undertakes the prosecution.

Article 508

(1) The request by the foreign country in the Republic of Macedonia to be undertaken prosecution of a citizen of the Republic of Macedonia or of a person who has a residence in the Republic of Macedonia for a crime committed abroad, is directed with the records to the competent public prosecutor on whose region the person has his residence.
(2) If to the competent agency of the foreign country is submitted the lawful property request, it will be proceeded as if the request is submitted to the competent court.
(3) Of the refusal the criminal prosecution to be undertaken as well as whether the decision is legally valid, which has been brought in the criminal procedure, will be informed the foreign country which has submitted the request.

6.2.28 Turkey

(IV) THE RELEVANT TURKISH LEGISLATION ON JUDICIAL COOPERATION IN CRIMINAL MATTERS:

1. Constitution:

In the Constitution, there are two provisions related to judicial cooperation in criminal matters.
Article 90 regulates the relationship between the laws and international agreements inter alia on judicial cooperation in criminal matters.

Under Article 90, international agreements duly put into effect carry the force of law.
In accordance with Article 90, once an international agreement has been ratified, it becomes internal part of the national legal system and can directly be enforced.
No appeal to the Constitutional Court can be made with regard to these agreements on the ground that they are unconstitutional.
Article 38 of the Constitution provides that citizens shall not be extradited to a foreign country on account of an offence except under obligations resulting from being a party to the International Criminal Court.

2. Code and Laws:

There is no specific law on judicial cooperation in criminal matters but the following laws include some provisions on judicial cooperation in criminal matters:
a) Turkish Criminal Code (TCC), Law no: 5237, dated September 26, 2004, Article 18 governs extradition:
b) Law on the Organization and Functions of the Ministry of Justice (Law No. 2992):
Article 13/A of this Law provides that General Directorate for International Law and Foreign Relations is the central authority for execution of all kinds of judicial assistance requests in criminal matters.

3. International Agreements:

The main sources of international judicial cooperation in criminal matters in Turkey are the bilateral agreements between Turkey and other countries and the multilateral agreements to which Turkey is a party.
Multilateral Conventions of the Council of Europe and United Nations to which Turkey is a party.

Turkey is a party to "OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions" dated 21 November 1997. On the other hand Turkey is a member of "The Financial Action Task Force (FATF)" that is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

If there is no bilateral and multilateral convention between Turkey and other country concerned, judicial cooperation in criminal matters is governed by international customs and principle of reciprocity.

4. Circulars

The subjects on the implementation of judicial cooperation in criminal matters are governed by the circulars issued by the General Directorate for the International Law and Foreign Relations of the Ministry of Justice.
As the recent TCC and TCPC came into force on 1 June 2005, a new circular no: 69 and dated 1/1/2006 has been issued. Mainly following issues are covered in this circular:
-Service of documents and letters rogatory including mutual legal assistance on the enforcement of the decisions on seizure and confiscation,
-Extradition, requests for search of offenders with Interpol Red Notice,
-Transfer of sentenced persons,
-Researches of addresses in abroad and provision of birth and death certificates and judicial records of foreign nationals.

(V) JUDICIAL COOPERATION IN PRACTICE

1. Mutual Legal Assistance

Turkey does not have any legislation that specifically deals with MLA. Bilateral and multilateral conventions are the main instruments in MLA practice in Turkey. The Ministry of Justice of Turkey plays a central role in judicial co-operation at large. General Directorate of International Law and Foreign Relations as a central authority receives the requests for mutual legal assistance and then transmits them to the competent authorities for execution. According to the general legal system, the competent authority may be either the court or the public prosecutor depending on the type of the assistance sought.

In cases of urgent requests under article 15 of the 1959 Convention (i.e. via Interpol), the Ministry of Interior will transmit the request to the Ministry of Justice for execution. Turkey has a positive approach to judicial co-operation, more precisely; incoming requests are carried out in a flexible and a cooperative manner. Turkey carries out requests of mutual assistance in criminal matters basically within the framework of "European Convention on Mutual Assistance in Criminal Matters."

6.2.29 Ukraine

Articles of CPC of Ukraine

CPC Article 159 Temporary access to objects or documents

1. Temporary access to the objects and documents means ability of the party of the criminal procedure on the will of the legal owner of some object or thing to operate with them, making copies and reading. Upon receiving warrant of investor-judge or judge – seize them.
2. Temporary access to the objects and documents can be carried out upon award of the investigator-judge or judge.

CPC Article 160 Petition on temporary access to objects and documents

1. Parties of the criminal procedure has a right to file a motion to investigator-judge or judge on the issue of temporary access to objects and documents, accept of the exclusions pointed in Article 161 of this Code. Investigator is empowered to file mentioned motion to investigator-judge that is approved by prosecutor.
2. Petition should contain:
- capsule review of the factual background of the criminal misdemeanor;
- legal qualification of the criminal misdemeanor according the Article in the Penal Code;
- objects and documents that are objectives of the temporary access procedure;
- grounds to believe that objects and things that need to be temporary accessed are owned by some person;
- objects and documents have a considerable value to identification of circumstances in criminal proceedings;
- ability to use information that can be received from objects and documents as evidence and impossibility to gain the given evidence in other way but by temporary access to objects and things;
- explanation of necessity to seize objects and things if the given issue is initiated by the party of criminal process.

CPC Article 161 Objects and things access to which is denied

1. Objects and things the access to which is denied:
- correspondence and other forms of data changing between attorney and his client or any other person that represents clients' law interests;
- objects attached to the given correspondence or other forms or data changing.

CPC Article 162 Objects and things that include secret data protected by law

Data that contains secret and stored in objects and documents is the following:
- information that belongs to mass media agencies or reporters that was given them on the basis of secrecy without uncovering source of its receiving;
- information that may contain doctor's secret;
- information that may contain notaries acts;
- confidential information including commercial data;
- information that can contain banking data;
- private correspondence of the person and other data of private character;
- information that is stored on the equipment of operators and telecommunication providers: connection, prescriber, the fact of access to the net, connection duration, content, routes of transmitting the data, etc;
- personal data that is stored in smb's private database or database that is possessed by the owner of the personal data;
- state secret.

CPC Article 163 Review of petition on temporary access to objects and things

1. Upon receiving petition on temporary access to objects and things investigator-judge or judge subpoenas holder (=owner) of objects and things that need to be temporary accessed accept of the case described by section 2 Article 163.
2. If the party of the criminal process that applied with petition proves sufficient grounds to regard the possible change or loss, or elimination of objects and documents, the mentioned petition can be reviewed by investigator-judge or judge without subpoena of the holder of objects and things.
3. Subpoena letter that is sent to the object/document owner contains provisions to retain data as it is from the time the letter was received.
4. Investigator-judge or judge that reviews petition on temporary access to objects and things in presence of the petition's initiator as well as holder of objects and documents. Scheduled review of the petition will be conducted not looking on the fact whether holder of objects and things is present or not.
5. Investigator-judge, judge serves warrant on temporary access to objects and things if it is proved that they:
- locate or can locate within the property of natural or legal person;
- bear distinctive meaning for identifying circumstances in criminal proceedings;
- does not include secret that is under protection of law.
6. Investigator-judge or judge also serves a warrant on giving permission for temporary access to objects and things when it is proven that the data stored on them might be used as evidence and that there is no other legal way to prove some circumstances of the criminal proceedings.
Access to law-protected information that is stored on objects and things is regulated by law. State secret data cannot be accessed by the person that has no right on it.
7. Investigator-judge, judge can also give an order to seize objects and things in case the party of the criminal process proves that there is a threat that they can be changed, deleted or lost.

Article 551 (Request for international assistance) says the following:

1. Judge, prosecutor or investigator with prior prosecutor's approval sends to the competent (central) body* of Ukraine request on international assistance within the scope of criminal proceeding that is being carried out.
2. Competent (central) body regards the received request in view of compliance to domestic laws and signed international treaties.
3. Upon positive decision competent (central) body sends a request to the competent body of requested Party within 10 days directly or through diplomatic channels.
4. Upon negative decision all the documents should be returned to the initiator within 10 days enlisting failings and mistakes.
* - General Prosecutor's Office

Article 552 Content and forms of request for mutual legal assistance

1. Content and forms of request for mutual legal assistance should correspond to the provisions of CPC of Ukraine or international treaty sighed by Ukraine. Request must be composed in the form of procuratory.
2. Request should contain:
- name of the requesting official body and competent body of requested Party;
- reference on international treaty for mutual legal assistance signed by Parties;
- name of criminal proceeding according to which the request is sent;
- capsule review of the criminal proceeding and its legal qualification;
- data about person, her full name, DOB, place of residence, citizenship, her procedural status and her liaison to the subject of criminal procedure;
- accurate list of needed procedural actions to be committed and their justification;
- persons that should be present during procedural actions and justification of this necessity;
- other information that can facilitate the obtaining of requested data.

3. Request must also contain a roster of Articles of domestic criminal legislation with the purpose to read rights and obligations of person who will interrogated as witness, expert, victim, suspect or accused. Request should also be accompanied with questions that must be put before mentioned persons.
4. Request on conducting searches, inspecting the crime scene, seize, arrest or confiscation of things should be carried out according to the requirements of this CPC.
5. It not compulsory to include into request data enlisted in sub-paras 4, 5, 8 of the para 2 of this Article.
6. While the request for mutual legal assistance is on pretrial stage, it should be approved by prosecutor who is in charge for controlling compliance with laws of pretrial investigation.

Article 557 of CPC Refusal on execution of request for mutual assistance

1. Requesting party may be refused in execution of request for mutual assistance in cases that are provided by international treaties that are signed by Ukraine.
2. While there are no international treaty with requesting Party, the initiator can be refused in execution of request for mutual assistance in the following cases:
- if the requests contradict Ukrainian Constitution and can harm sovereignty, security, public order, or other Ukrainian interests;
- if the requests refer to person who'd been already judged and court's decision came into effect;
- the requesting party does not support mutual law enforcement assistance when needed;
- request refers to the criminal misdemeanor that is not punishable due to the domestic laws;
- there are grounds to think that request is aimed to pursue persons because of their race, color of their skin, political, religious beliefs, sex, ethnic or social origin, property status, place of residence, or linguistic or other signs;
- request concerns the criminal misdemeanor or offense that is currently a subject of pretrial investigation or trial.

6.2.30 United Kingdom

Crime (International Co-operation) Act 2003.

Art. 7 Requests for assistance in obtaining evidence abroad

(1) If it appears to a judicial authority in the United Kingdom on an application made by a person mentioned in subsection (3)—

(a) that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted or that the offence is being investigated,

the judicial authority may request assistance under this section.

(2) The assistance that may be requested under this section is assistance in obtaining outside the United Kingdom any evidence specified in the request for use in the proceedings or investigation.

(3) The application may be made—

(a) in relation to England and Wales and Northern Ireland, by a prosecuting authority,

(b) in relation to Scotland, by the Lord Advocate or a procurator fiscal,

(c) where proceedings have been instituted, by the person charged in those proceedings.

(4) The judicial authorities are—

(a) in relation to England and Wales, any judge or justice of the peace,

(b) in relation to Scotland, any judge of the High Court or sheriff,

(c) in relation to Northern Ireland, any judge or resident magistrate.

(5) In relation to England and Wales or Northern Ireland, a designated prosecuting authority may itself request assistance under this section if—

(a) it appears to the authority that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) the authority has instituted proceedings in respect of the offence in question or it is being investigated.

- "Designated" means designated by an order made by the Secretary of State.

(6) In relation to Scotland, the Lord Advocate or a procurator fiscal may himself request assistance under this section if it appears to him—

(a) that an offence has been committed or that there are reasonable grounds for suspecting that an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted or that the offence is being investigated.

(7) If a request for assistance under this section is made in reliance on Article 2 of the 2001 Protocol (requests for information on banking transactions) in connection with the investigation of an offence, the request must state the grounds on which the person making the request considers the evidence specified in it to be relevant for the purposes of the investigation.

Art. 8 Sending requests for assistance

(1) A request for assistance under section 7 may be sent—

(a) to a court exercising jurisdiction in the place where the evidence is situated, or

(b) to any authority recognised by the government of the country in question as the appropriate authority for receiving requests of that kind.

(2) Alternatively, if it is a request by a judicial authority or a designated prosecuting authority it may be sent to the Secretary of State (in Scotland, the Lord Advocate) for forwarding to a court or authority mentioned in subsection (1).

(3) In cases of urgency, a request for assistance may be sent to—

(a) the International Criminal Police Organisation, or

(b) any body or person competent to receive it under any provisions adopted under the Treaty on European Union,

for forwarding to any court or authority mentioned in subsection (1).

Art. 13 Requests for assistance from overseas authorities

(1) Where a request for assistance in obtaining evidence in a part of the United Kingdom is received by the territorial authority for that part, the authority may—

(a) if the conditions in section 14 are met, arrange for the evidence to be obtained under section 15, or

(b) direct that a search warrant be applied for under or by virtue of section 16 or 17 or, in relation to evidence in Scotland, 18.

(2) The request for assistance may be made only by—

(a) a court exercising criminal jurisdiction, or a prosecuting authority, in a country outside the United Kingdom,

(b) any other authority in such a country which appears to the territorial authority to have the function of making such requests for assistance,

(c) any international authority mentioned in subsection (3).

(3) The international authorities are—

(a) the International Criminal Police Organisation,

(b) any other body or person competent to make a request of the kind to which this section applies under any provisions adopted under the Treaty on European Union.

Art. 14 Powers to arrange for evidence to be obtained

(1) The territorial authority may arrange for evidence to be obtained under section 15 if the request for assistance in obtaining the evidence is made in connection with—

(a) criminal proceedings or a criminal investigation, being carried on outside the United Kingdom,

(b) administrative proceedings, or an investigation into an act punishable in such proceedings, being carried on there,

(c) clemency proceedings, or proceedings on an appeal before a court against a decision in administrative proceedings, being carried on, or intended to be carried on, there.

(2) In a case within subsection (1)(a) or (b), the authority may arrange for the evidence to be so obtained only if the authority is satisfied—

(a) that an offence under the law of the country in question has been committed or that there are reasonable grounds for suspecting that such an offence has been committed, and

(b) that proceedings in respect of the offence have been instituted in that country or that an investigation into the offence is being carried on there.

An offence includes an act punishable in administrative proceedings.

(3) The territorial authority is to regard as conclusive a certificate as to the matters mentioned in subsection (2)(a) and (b) issued by any authority in the country in question which appears to him to be the appropriate authority to do so.

(4) If it appears to the territorial authority that the request for assistance relates to a fiscal offence in respect of which proceedings have not yet been instituted, the authority may not arrange for the evidence to be so obtained unless—

(a) the request is from a country which is a member of the Commonwealth or is made pursuant to a treaty to which the United Kingdom is a party, or

(b) the authority is satisfied that if the conduct constituting the offence were to occur in a part of the United Kingdom, it would constitute an offence in that part.

for forwarding to any court or authority mentioned in subsection (1).

Art. 19 Seized evidence

(1) Any evidence seized by a constable under or by virtue of section 16, 17 or 18 is to be sent to the court or authority which made the request for assistance or to the territorial authority for forwarding to that court or authority.

(2) So far as may be necessary in order to comply with the request for assistance—

(a) where the evidence consists of a document, the original or a copy is to be sent, and

(b) where the evidence consists of any other article, the article itself or a description, photograph or other representation of it is to be sent.

(3) This section does not apply to evidence seized under or by virtue of section 16(2)(b) or (4)(b) or 18(2)(b).

Art. 24 Evidence seized under the order

(1) Any evidence seized by or produced to the constable under section 22 is to be retained by him until he is given a notice under subsection (2) or authorised to release it under section 25.

(2) If—

(a) the overseas freezing order was accompanied by a request for the evidence to be sent to a court or authority mentioned in section 13(2), or

(b) the territorial authority subsequently receives such a request,

the territorial authority may by notice require the constable to send the evidence to the court or authority that made the request.

25 Release of evidence held under the order

(1) On an application made by a person mentioned below, the nominated court may authorise the release of any evidence retained by a constable under section 24 if, in its opinion—

(a) the condition in section 21(6) or (7) is met, or

(b) the overseas freezing order has ceased to have effect in the participating country.

(2) In relation to England and Wales and Northern Ireland, the persons are—

(a) the chief officer of police to whom a copy of the order was sent,

(b) the constable,

(c) any other person affected by the order.

(3) In relation to Scotland, the persons are—

(a) the procurator fiscal to whom a copy of the order was sent,

(b) any other person affected by the order.

(4) If the territorial authority decides not to give a notice under section 24(2) in respect of any evidence retained by a constable under that section, the authority must give the constable a notice authorising him to release the evidence.

6.2.31 United States

Title 18, U.S.C., Section 3512

(a) **Execution of Request for Assistance.—**
(1) **In general.—** Upon application, duly authorized by an appropriate official of the Department of Justice, of an attorney for the Government, a Federal judge may issue such orders as may be necessary to execute a request from a foreign authority for assistance in the investigation or prosecution of criminal offenses, or in proceedings related to the prosecution of criminal offenses, including proceedings regarding forfeiture, sentencing, and restitution.
(2) **Scope of orders.—** Any order issued by a Federal judge pursuant to paragraph (1) may include the issuance of—
(A) a search warrant, as provided under Rule 41 of the Federal Rules of Criminal Procedure;
(B) a warrant or order for contents of stored wire or electronic communications or for records related thereto, as provided under section 2703 of this title;
(C) an order for a pen register or trap and trace device as provided under section 3123 of this title; or
(D) an order requiring the appearance of a person for the purpose of providing testimony or a statement, or requiring the production of documents or other things, or both.

(b) **Appointment of Persons To Take Testimony or Statements.—**
(1) **In general.—** In response to an application for execution of a request from a foreign authority as described under subsection (a), a Federal judge may also issue an order appointing a person to direct the taking of testimony or statements or of the production of documents or other things, or both.
(2) **Authority of appointed person.—** Any person appointed under an order issued pursuant to paragraph (1) may—
(A) issue orders requiring the appearance of a person, or the production of documents or other things, or both;
(B) administer any necessary oath; and
(C) take testimony or statements and receive documents or other things.

(c) **Filing of Requests.—** Except as provided under subsection (d), an application for execution of a request from a foreign authority under this section may be filed—
(1) in the district in which a person who may be required to appear resides or is located or in which the documents or things to be produced are located;
(2) in cases in which the request seeks the appearance of persons or production of documents or things that may be located in multiple districts, in any one of the districts in which such a person, documents, or things may be located; or
(3) in any case, the district in which a related Federal criminal investigation or prosecution is being conducted, or in the District of Columbia.

(d) **Search Warrant Limitation.—** An application for execution of a request for a search warrant from a foreign authority under this section, other than an application for a warrant issued as provided under section 2703 of this title, shall be filed in the district in which the place or person to be searched is located.

(e) **Search Warrant Standard.—** A Federal judge may issue a search warrant under this section only if the foreign offense for which the evidence is sought involves conduct that, if committed in the United States, would be considered an offense punishable by imprisonment for more than one year under Federal or State law.

(f) **Service of Order or Warrant.—** Except as provided under subsection (d), an order or warrant issued pursuant to this section may be served or executed in any place in the United States.

(g) **Rule of Construction.—** Nothing in this section shall be construed to preclude any foreign authority or an interested person from obtaining assistance in a criminal investigation or prosecution pursuant to section 1782 of title 28, United States Code.

(h) **Definitions.—** As used in this section, the following definitions shall apply:

(1) **Federal judge.—** The terms "Federal judge" and "attorney for the Government" have the meaning given such terms for the purposes of the Federal Rules of Criminal Procedure.

(2) **Foreign authority.—** The term "foreign authority" means a foreign judicial authority, a foreign authority responsible for the investigation or prosecution of criminal offenses or for proceedings related to the prosecution of criminal offenses, or an authority designated as a competent authority or central authority for the purpose of making requests for assistance pursuant to an agreement or treaty with the United States regarding assistance in criminal matters.

6.3 Extraits de la Convention de Budapest sur la cybercriminalité

Article 31 – Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Rapport explicatif

Entraide concernant l'accès aux données stockées (article 31)

292. Chaque partie doit avoir la capacité, au bénéfice de l'autre, de perquisitionner ou d'accéder par un moyen similaire, de saisir ou d'obtenir par un moyen similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire – tout comme elle doit, en vertu de l'article 19 (Perquisition et saisie de données informatique stockées), avoir la capacité de le faire à des fins nationales. Le paragraphe 1 autorise une Partie à demander ce type d'entraide et le paragraphe 2 exige de la Partie requise qu'elle se donne les moyens de la fournir. Par ailleurs, le paragraphe 2 est conforme au principe selon lequel les conditions dans lesquelles cette coopération doit être fournie sont celles qu'énoncent les traités, arrangements et législations nationales applicables concernant l'entraide judiciaire en matière pénale. En vertu du paragraphe 3, il doit être satisfait rapidement à une telle demande lorsque 1) il y a des raisons de penser que les données pertinentes sont particulièrement susceptibles de perte ou de modification, ou 2) les traités, arrangements ou législations prévoient une coopération rapide.

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Article 25 – Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2. a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution;

b. Les autorités centrales communiquent directement les unes avec les autres;

c. Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise:

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a. En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b. Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour

des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande:
a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Article 35 – Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

a. apport de conseils techniques;
b. conservation des données, conformément aux articles 29 et 30;
c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.