COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Projet
15 mai 2017
Strasbourg, France

T-CY (2017)2

Comité de la Convention cybercriminalité (T-CY)

Rapport d'évaluation sur l'entraide judiciaire :

Suites données aux Recommandations par les Parties et les Observateurs

Projet préparé par le Bureau du T-CY pour examen par le T-CY 17 (juin 2017)

www.coe.int/TCY

Table des matières

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

1 Historique

Une entraide judiciaire rapide est l'une des conditions les plus importantes pour obtenir des mesures efficaces contre la criminalité et d'autres infractions impliquant des preuves électroniques, étant donné le caractère transnational et volatile de ces dernières. En pratique, cependant, les procédures d'entraide judiciaire sont considérées trop complexes, prenant trop de temps et mobilisant trop de ressource, 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, en concentrant l'évaluation sur l'article 31 de la Convention 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.
>
> 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.

L'évaluation s'est achevée par l'adoption du Rapport d'évaluation lors de la 12e Réunion Plénière du T-CY les 2-3 décembre 2014[1].

Le Rapport comprend une série de Recommandations tombant sous la responsabilité des Parties :

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 des données (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 (comme 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.

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

Rec 5	Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact 24/7 conformément à l'article 35 de la Convention de Budapest, notamment : a. veiller, conformément à l'article 35.3 de la 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 parmi les autorités nationales et leurs homologues étrangères ; c. assurer entre les Parties 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'État 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 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. À cet égard, les Parties doivent partager les bonnes pratiques avec le T-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 services.
Rec 9	Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.
Rec 10	Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide judiciaire.
Rec 11	Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.
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 de la 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 pour faciliter 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.

Les Parties ont été invitées à donner suite aux Recommandations relevant de leur responsabilité et à rendre compte au T-CY dans les 18 mois des mesures prises, conformément au Règlement intérieur du T-CY (article 2.1.g), pour examiner les progrès réalisés.

Suite à la décision du T-CY 15 (24-25 mai 2016) d'« inviter le Bureau à préparer et au Secrétariat à diffuser une demande d'information sur les suites données aux Recommandations 1 à 7 et 9 à 15 du Rapport d'évaluation sur l'entraide judiciaire, ainsi que sur la Recommandation 16

concernant la période de conservation des données », un questionnaire élaboré par le Bureau du T-CY a été envoyé à toutes les Parties le 16 septembre 2016, le délai pour les réponses étant fixé au 21 octobre 2016. À cette date, 18 Parties avaient répondu au questionnaire.

Le T-CY 16 (14-15 novembre 2016) a décidé « d'accueillir favorablement les réponses au questionnaire sur les suites données par les 18 Parties et d'inviter les Parties et les Observateurs qui ne l'ont pas encore fait à adresser leurs réponses au plus tard le 15 décembre 2016 ».

Au 30 avril 2017, 40 Parties avaient répondu au questionnaire:

Albanie
Allemagne
Arménie
Australie
Autriche
Azerbaïdjan
Belgique
Bosnie et Herzégovine
Bulgarie
Canada
Croatie
Danemark
Espagne
Estonie
États-Unis d'Amérique
Finlande
France
Hongrie
Israël
Italie
Japon
Lettonie
Liechtenstein
Lituanie
Malte
Maurice
Moldova
Monténégro
Norvège
Pays-Bas
Pologne
Portugal
République dominicaine
République tchèque
Roumanie
Serbie
Slovaquie
Slovénie
Suisse
Turquie

2 Suites données par les Parties aux Recommandations 1 à 15

2.1 Rec 1 – Mise en œuvre des dispositions de la Convention de Budapest

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 des données (suite au Rapport d'évaluation de 2012 du T-CY).

2.1.1 Aperçu général des suites données à la Recommandation

Cette Recommandation résultait de la conviction des Parties que la pleine mise en œuvre des dispositions relatives à la coopération procédurale internationale figurant dans la Convention de Budapest aiderait grandement à obtenir des éléments de preuve au niveau international.

La plupart des États répondants affirment qu'ils appliquent les dispositions de la Convention[2]. Certains États indiquent spécifiquement que leur législation contient une disposition sur la conservation des données (Albanie, Arménie, Australie, Canada, Croatie, Espagne, États-Unis, Finlande, Japon, Lettonie, Lituanie, Malte, Moldova, Monténégro, Norvège, Pays-Bas, Pologne, Portugal, Roumanie, Slovaquie) [3].

Certains États qui ne se sont pas dotés d'une disposition légale sur la conservation des données s'appuient sur les pouvoirs implicites d'application de la loi pour décider des mesures de conservation des données (Bulgarie, Estonie, France). D'autres envisagent d'introduire une disposition à ce sujet dans la loi ou la réglementation (Azerbaïdjan, Italie, Slovénie).

Quelques États exigent l'entraide judiciaire pour appliquer des mesures de conservation des données ou ne sont pas autrement en pleine conformité avec la Convention (Hongrie, Maurice, République tchèque, Serbie, Turquie)[4]. D'autres travaillent actuellement à renforcer leur conformité avec la Convention (Bosnie et Herzégovine, Liechtenstein).

2.1.2 Exemples de bonnes pratiques

De nombreux États suivent la bonne pratique consistant à introduire une disposition spécifique sur la conservation des données dans le droit interne afin de permettre l'exécution de mesures de préservation de façon simple et rapide et sans qu'une décision d'un tribunal soit nécessaire.

2.1.3 Conclusion

Les dispositions relatives à la coopération procédurale internationale de la Convention de Budapest sont essentielles pour obtenir des éléments de preuve au niveau international et devraient être pleinement mises en œuvre. L'imposition de mesures de conservation des données constitue, en particulier, un outil fondamental, fréquemment utilisé et peu intrusif. Les Parties devraient supprimer les obstacles à l'application facile de mesures de conservation et envisager fortement d'adopter une disposition écrite à ce sujet.

---

[2] Chypre, la Géorgie, l'Islande, le Luxembourg, Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question.

[3] Pour une analyse détaillée de la mise en œuvre des dispositions relatives à la conservation, voir les rapports du Comité sur la Convention cybercriminalité (T-CY) :

- Rapport d'évaluation sur la mise en œuvre des dispositions de la Convention de Budapest en matière de conservation des données

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e

- Rapport d'évaluation supplémentaire sur la mise en œuvre des dispositions en matière de conservation des données

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

[4] La République tchèque envisage d'adopter une législation visant à simplifier la procédure de traitement des demandes étrangères de conservation de preuves. Cependant, seules les Parties à la Convention de Budapest pourront bénéficier de cette procédure simplifiée et non les autres États.

2.2 Rec 2 – Statistiques et suivi de l'efficience de l'entraide judiciaire

> 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.

2.2.1 Aperçu général des suites données à la Recommandation

Avec cette Recommandation, les Parties voulaient signaler que les données concrètes sur la charge de travail croissante posée par les preuves électroniques – au lieu de procédures globales – devraient alerter les décideurs et conduire éventuellement à l'allocation de ressources plus importantes aux bureaux chargés de la « cyber-entraide judiciaire ».

De nombreux États tiennent des statistiques sur la cyber-entraide judiciaire[5], peuvent interroger les bases de données existantes pour obtenir de telles statistiques ou se sont dotés de nouveaux systèmes de documentation et de gestion des affaires qui rendent possible la tenue de statistiques (Albanie, Australie, Azerbaïdjan, Belgique, Bulgarie, Canada, Croatie, Espagne, États Unis, Hongrie, Italie, Lituanie, Malte, Maurice, Moldova, Monténégro, Roumanie,[6] Serbie, Slovaquie, Slovénie, Suisse, Turquie). D'autres travaillent actuellement au développement de systèmes de ce type (Bosnie et Herzégovine, Finlande, Pays-Bas, République tchèque).

Certains États déclarent que ces statistiques n'existent pas ou que leur tenue n'est pas possible (Arménie, Autriche, Danemark, France[7], Israël, Liechtenstein, Norvège, Pologne). Au Liechtenstein, le volume des affaires à traiter n'est pas très élevé et une base de données n'est pas nécessaire pour évaluer l'efficience.

Le Portugal indique qu'il n'est pas possible de tenir des statistiques précises sur la cyber-entraide judiciaire parce que la coopération directe entre autorités judiciaires ne passe pas par un point de contrôle central. De nombreux États soulignent l'importance de la coopération directe, qui est fortement utilisée entre les États membres de l'UE, pour améliorer la cyber-coopération. Il serait intéressant de voir si d'autres États s'appuyant sur des contacts directes rencontrent eux aussi le problème soulevé par le Portugal.

2.2.2 Exemples de bonnes pratiques

Australie : l'autorité centrale tient une base de données sur toutes les affaires d'entraide judiciaire, y compris celles qui portent sur la cybercriminalité et impliquent des preuves électroniques. Cette base de données lui permet de produire des statistiques sur le nombre d'affaires, ventilées par pays d'origine, type d'infraction et type d'aide requise. L'Autorité centrale passe actuellement en revue ses normes de gestion des dossiers en vue de développer une nouvelle base de données plus performante. Elle contrôle et examine continuellement les pratiques de traitement des dossiers du point de vue de la réactivité et de l'efficience.

Malte : l'Office de l'Attorney General dispose d'une base de données qui conserve des informations statistiques sur toutes les requêtes d'entraide judiciaire reçues et envoyées, y compris celles qui portent sur la cybercriminalité et reposent sur des preuves électroniques.

---

[5] L'Allemagne, Chypre, la Géorgie, l'Islande, la Lettonie, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question.

[6] La Roumanie – via le bureau du procureur au stade de l'enquête – tient des statistiques uniquement sur l'entraide judiciaire concernant la cybercriminalité et non sur l'entraide judiciaire concernant les preuves électroniques.

[7] La France peut obtenir le nombre d'affaires traitées par l'autorité centrale mais non spécifiquement le nombre d'affaires concernant la cybercriminalité et les preuves électroniques.

Moldova : le Bureau du Procureur général tient des statistiques sur toutes les requêtes d'entraide judiciaire, y compris celles portant sur la cybercriminalité. Avec le Département des technologies de l'information et de lutte contre la cybercriminalité, le Bureau du Procureur général assure le suivi rigoureux des requêtes concernant la cybercriminalité.

Monténégro : l'autorité centrale utilise un système de gestion électronique des requêtes d'entraide judiciaire. Elle peut ainsi disposer de données statistiques ventilées selon différents critères comme, par exemple, le type d'infraction pénale, le type d'entraide judiciaire ou l'État requérant.

Suisse : les statistiques sont publiées en ligne (les liens sont fournis).

États-Unis : l'autorité centrale tient une base de données sur toutes les requêtes d'entraide judiciaire qu'elle reçoit en vue de l'obtention de preuves électroniques (qu'il s'agisse d'une requête électronique ou sur papier). La base de données enregistre, entre autres choses, la durée de la requête, les communications de et vers l'État requérant et la résolution de chaque affaire. Le système peut aussi produire des statistiques et analyser les tendances concernant ce type de requêtes.

2.2.3 Conclusion

Il semble que la plupart des États soient en mesure de produire au moins certaines statistiques sur la cyber-coopération. Il serait intéressant de voir si ces statistiques confirment l'impression des praticiens de la lutte contre la cybercriminalité, à savoir que le système est lent et surchargé. D'autre part, le T-CY pourrait examiner la possibilité d'utiliser de quelque façon des statistiques agrégées. Il serait également utile de partager les statistiques existantes avec le T-CY.[8]

[8] N.B. : Pendant l'évaluation réalisée par le T-CY, très peu de Parties ont fourni des données statistiques.

2.3 Rec 3 – Affectation de ressources

> 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 (comme les Bureaux locaux des procureurs).

2.3.1 Aperçu général des suites données à la Recommandation

Cette Recommandation reposait sur l'idée que la procédure d'entraide judiciaire peut être ralentie où même bloquée si les agents impliqués dans le processus de coopération judiciaire ne sont pas familiarisés avec la technologie en cause dans une affaire. Ils risquent en pareil cas de ne pas poser les bonnes questions ou de ne pas fournir le travail requis pour soutenir ou accélérer le traitement d'une requête d'entraide judiciaire.

Les Parties prennent en général au sérieux les problèmes signalés dans cette Recommandation. La plupart travaillent à les résoudre, principalement par la formation, la mise en place de liens spéciaux et l'emploi d'un personnel spécialisé[9]. Ces trois approches sont fréquemment utilisées concurremment.

Les États sont classés ci-dessous en gros sur la base des points principaux mis en avant dans leurs réponses. Ce classement ne signifie pas que les États concernés ne prennent aucune autre mesure. Il semble au contraire que chacun de ces États teste différentes méthodes pour répandre et approfondir les connaissances techniques.

Les Parties mentionnent spécifiquement :

- La formation des agents travaillant dans le secteur de la cyber-coopération judiciaire : Australie, Belgique, Bulgarie, Finlande.
- Le travail en réseau ou l'établissement de liens spéciaux entre les bureaux pertinents, par exemple les bureaux des procureurs chargés de la cyber-coopération judiciaire et la cyber-police nationale : Allemagne, Autriche, Hongrie, Liechtenstein, Malte, République dominicaine, Slovaquie.
- L'utilisation de personnel spécialisé : Albanie, Azerbaïdjan, Canada, Danemark, Estonie, États-Unis, France, Israël, Japon, Lituanie, Maurice, Moldova, Norvège, République tchèque, Roumanie, Suisse, Turquie.

D'autres États examinent actuellement ces questions, mettent l'accent sur la formation spécialisée au sein des bureaux des procureurs locaux ou recrutent un personnel formé aux technologies (Bosnie et Herzégovine, Finlande, Pologne, Serbie).

2.3.2 Exemples de bonnes pratiques

Australie : l'autorité centrale forme ses agents au moment de leur entrée dans l'emploi, puis ensuite pour les aider à se tenir à jour de l'évolution des technologies et, en particulier, de la manière dont elles sont utilisées à des fins criminelles.

[9] Chypre, la Croatie, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. Le Portugal a indiqué n'avoir pris aucune mesure spécifique.

Autriche : la coopération entre les procureurs et la cyber-police de l'office central de la police est rapide, souple et efficiente. En outre, chaque tribunal régional dispose d'un personnel technique prêt à apporter son soutien.

Azerbaïdjan : les requêtes de cyber-coopération judiciaire sont traitées par un personnel formé aux technologies, à la fois à l'échelon central et au sein des institutions chargées de l'exécution des requêtes.

France : de nombreux organes du gouvernement français (y compris l'autorité centrale, à Paris, à Lille et ailleurs) comprennent des magistrats, des fonctionnaires et des unités spécialisés dans la lutte contre la cybercriminalité, la collecte de preuves électroniques, la cyber-criminalistique et les cyber-enquêtes.

Israël : le Bureau du Procureur général inclut un département international, qui fonctionne comme autorité désignée sur les questions de droit et de technologie, et un département de lutte contre la cybercriminalité. Les membres de ce département se réunissent régulièrement avec leurs homologues étrangers et les représentants de plusieurs fournisseurs de services internet.

Japon : au sein du Bureau du Procureur général et des grands Bureaux des procureurs de district, des procureurs formés aux technologies sont chargés de traiter les affaires de cybercriminalité. Le ministère de la Justice cherche aussi à développer la capacité des procureurs à enquêter sur la cybercriminalité dans l'ensemble du pays en organisant des formations aux technologies utilisées dans la cybercriminalité et aux méthodes d'enquête électroniques. Dans les forces de police, tant au niveau national qu'à celui de chaque préfecture, des policiers formés aux technologies sont chargés des enquêtes sur la cybercriminalité.

Lituanie : Les demandes de cyber-coopération judiciaire sont traitées conjointement par des procureurs et des enquêteurs formés aux questions techniques et juridiques en jeu. Le travail technique de collecte des preuves est effectué par des cyber-enquêteurs chargés de la lutte contre la cybercriminalité au sein des divisions de la police nationale ou de l'une des dix forces de police locales. La division nationale de lutte contre la cybercriminalité traite normalement les affaires de criminalité organisée et les affaires transnationales importantes.

Suisse : des unités spéciales de lutte contre la cybercriminalité ont été créées au sein des bureaux des procureurs à l'échelon fédéral et cantonal. Le Bureau du Procureur général de la Confédération comprend aussi des procureurs spécialisés, ce qui permet l'accès aux connaissances juridiques et technologiques adéquates en matière de cybercriminalité dans les affaires de cyber-coopération judiciaire. Il existe aussi plusieurs plateformes qui permettent le transfert de connaissances spécialisées à l'intérieur de chaque canton et entre les cantons et les autorités confédérales.

États-Unis : dans le cadre de son projet de de modernisation de l'entraide judiciaire, l'autorité centrale des États-Unis a créé une cyber-unité dont les procureurs et le personnel de soutien s'occupent exclusivement à temps plein du traitement des requêtes de cyber-coopération judiciaire. L'autorité centrale collabore avec les procureurs fédéraux de l'ensemble du pays qui sont spécialisés dans les cyber-enquêtes et l'aident dans l'exécution des requêtes.

2.3.3 Conclusion

Bien que beaucoup de travail reste à faire, les États semblent s'efforcer sérieusement de développer les connaissances technologiques du personnel s'occupant de l'entraide judiciaire.

2.4 Rec 4 – Formation à l'entraide judiciaire

> 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.

2.4.1 Aperçu général des suites données à la Recommandation

Devant l'augmentation constante du nombre de requêtes internationales portant sur des preuves électroniques, les Parties ont recommandé de développer la formation spécialisée parmi un personnel de plus en plus nombreux. Les Parties considèrent que cela permettrait d'accélérer l'entraide judiciaire et d'améliorer l'efficience du processus.

Les Parties semblent prendre cette Recommandation au sérieux et s'efforcer de la mettre en œuvre sous des modalités diverses[10].

De nombreux États disposent d'écoles de formation des policiers, des procureurs et des juges. Dans le cadre de ces institutions, certains d'entre eux ont mis en place ou développent des activités de formation régulières ou occasionnelles sur :

- les cyber-connaissances en général et la cyber-coopération judiciaire (Azerbaïdjan, Belgique, Bosnie et Herzégovine, Bulgarie, Croatie, Danemark, États-Unis, Italie, Japon, Lettonie, Lituanie, Moldova, République tchèque, Roumanie, Serbie, Slovaquie, Suisse) ;
- la cyber-coopération judiciaire (Albanie, Estonie, Portugal) ;
- les cyber-connaissances en général (France, Monténégro, Norvège, Pays-Bas).

Bien que la formation aux cyber-connaissances en général ne soit pas identique à la formation à la cyber-coopération judiciaire, toute amélioration des connaissances technologiques facilitera le traitement de la cyber-coopération judiciaire.

D'autres États organisent des formations sur un seul de ces sujets ou les deux par d'autres voies que les écoles de formation existantes (Australie, Autriche, Canada, Espagne, Hongrie, Maurice, Slovénie).

Certains États se déclarent intéressés à accueillir des activités de formation ou envisagent de les organiser eux-mêmes (Finlande, Pologne, République dominicaine).

Nombre de requêtes d'entraide judiciaire portent principalement sur des données couvertes par la juridiction des États-Unis. C'est la raison pour laquelle divers organes américains, notamment l'autorité centrale, le FBI et la Division pénale du Département de la Justice chargée de la lutte contre la cybercriminalité et le vol de propriété intellectuelle, organisent à l'intention de leurs partenaires étrangers le plus possible de formations sur les moyens d'obtenir des preuves électroniques des États-Unis. Ces formations ont lieu à l'intérieur ou à l'extérieur des États-Unis ou par vidéo-conférence. Elles s'adressent aux juges, aux procureurs et aux policiers. Les États-Unis participent en outre aux formations organisées par Action globale sur la cybercriminalité (GLACY), l'Organisation des États américains, l'Office des Nations Unies contre la drogue et le crime, et d'autres organisations.

[10] Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question.

D'autres États indiquent que leurs activités de formation portent en partie sur l'obtention de données couvertes par la juridiction des États-Unis.

Beaucoup d'entre eux indiquent aussi qu'ils participent à des formations organisées au niveau multilatéral, notamment par le Conseil de l'Europe.

2.4.2 Exemples de bonnes pratiques

Belgique : une formation de base et une formation avancée sur la cybercriminalité, incluant la formation à l'entraide judiciaire, sont organisées chaque année. Les magistrats en formation sont tenus de suivre une formation de trois jours sur la coopération policière et judiciaire internationale qui couvre la coopération dans le domaine de la cybercriminalité et des preuves électroniques. Les autres magistrats ont aussi la possibilité de suivre cette formation.

République tchèque : l'Académie judiciaire organise régulièrement des formations. Un séminaire national de formation à l'entraide judiciaire s'adressant à tous les procureurs et les juges est organisé tous les ans. Les procureurs et juges spécialisés dans l'entraide judiciaire se réunissent respectivement deux fois et une fois par an. La formation normale dispensée aux juges et aux procureurs à l'Académie judiciaire inclut des séminaires traitant de la cybercriminalité, de la criminalité économique et d'autres crimes. Ces séminaires abordent généralement la question des requêtes d'entraide judiciaire propres à ce type d'affaires. Des formations sont aussi organisées régulièrement à l'intention des policiers et il est prévu de les intensifier et de les étendre. Le but est de standardiser les connaissances et les pratiques en matière de détection et d'enquête sur la cybercriminalité et d'échanger des bonnes pratiques. Les policiers qui passent un examen à l'issue d'une formation régulière peuvent obtenir un certificat de criminalistique.

Danemark : le Collège de la police est responsable du développement professionnel des policiers et le Directeur des poursuites pénales de celui des procureurs. Le Centre national de lutte contre la cybercriminalité (NC3) joue un rôle essentiel dans la formation des policiers et des procureurs à la lutte contre la cybercriminalité. La coopération entre ces trois entités et les représentants des districts de police a conduit à la mise en place d'un « Programme national sur la lutte contre la cybercriminalité, Niveau 1 » en 2015 et ensuite d'un programme de niveau 2. Les spécialistes du NC3 reçoivent eux-mêmes une formation d'abord via un programme d'introduction obligatoire de trois semaines, puis dans le cadre d'une formation avancée obligatoire.
Les spécialistes nationaux et les policiers qui remplissent les conditions requises peuvent suivre les formations de l'European Cybercrime Training and Education Group et de l'Agence de l'Union, et le programme de Master de l'University College Dublin. Différents personnels peuvent aussi suivre des formations techniques internes, ainsi que des formations externes, des séminaires, etc.

Lituanie : la formation et le développement professionnel font partie de la politique de cybersécurité lituanienne. La Lituanie participe activement aux formations organisées par les organes de l'UE et d'autres États, notamment le Royaume-Uni et les États-Unis. Des policiers suivent chaque année de telles formations. Le Bureau de la police criminelle a lancé en 2014 une formation spécialisée sur divers aspects de l'investigation des affaires de cybercriminalité, y compris l'entraide judiciaire, en ciblant le futur personnel des unités spécialisées de lutte contre la cybercriminalité dans dix commissariats de comté. Les bureaux des procureurs locaux organisent dans tout le pays, jusqu'à quatre fois par an, des formations concernant la cybercriminalité à l'intention du personnel spécialisé des services de répression et du système judiciaire. Le Bureau du Procureur général et le Bureau de la police criminelle devraient émettre bientôt à l'intention des procureurs des recommandations sur la lutte contre la cybercriminalité, qui porteront sur les qualifications juridiques, la coopération internationale, les techniques d'enquête et d'autres sujets connexes.

Portugal : la coopération internationale est normalement incluse dans la formation initiale et la formation continue des juges et des procureurs dispensée au Centre d'études judiciaires. Des modules portant sur la coopération internationale sont inclus dans le programme d'études initial ; des séminaires, des conférences et des ateliers traitant de divers aspects de la coopération internationale sont ensuite organisés régulièrement. Les juges et les procureurs sont légalement tenus de suivre au moins deux sessions de formation par an et certains d'entre eux participent à des événements relatifs à la coopération internationale.

Roumanie et Slovaquie : les deux pays conduisent, institutionnalisent et participent à divers programmes, conférences et autres événements très détaillés pour les policiers, les procureurs et les juges. Ces événements portent entre autres sur la lutte contre la cybercriminalité, la coopération internationale et l'obtention de preuves couvertes par la juridiction des États-Unis. Des programmes de formation sont sponsorisés par les autorités nationales, en particulier l'académie judiciaire, et par de nombreuses organisations internationales, États partenaires et organisations universitaires.

2.4.3 Conclusion

Les États accordent une place de plus en plus importante à la formation de toutes les catégories d'agents publics impliqués dans la collecte et l'échange de preuves électroniques. Dans la poursuite de leurs efforts en ce domaine, les États devraient examiner la fréquence des formations, leur caractère régulier et obligatoire ou optionnel, et le fait de savoir si elles sont dispensées aux bonnes personnes et à un nombre de professionnels suffisant. Bref, les États devraient examiner la possibilité d'adopter une approche systématique de la formation.

2.5 Rec 5 – Points de contact 24/7

Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact 24/7 conformément à l'article 35 de la Convention de Budapest, notamment :

a. veiller, conformément à l'article 35.3 de la 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 parmi les autorités nationales et leurs homologues étrangères ;
c. assurer entre les Parties 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'État 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 un rôle de soutien pour les demandes « article 31 ».

2.5.1 Aperçu général des suites données à la Recommandation

Cette Recommandation avait pour but d'encourager l'adoption par les États de mesures concrètes qui, pour l'essentiel, relèvent de leurs compétences.

Presque tous les États ont pris des mesures en réponse à la Recommandation[11] et la quasi-totalité d'entre eux déclarent qu'ils veillent à assurer la présence de personnel formé et équipé pour faciliter le travail opérationnel et conduire ou soutenir les activités liées à l'entraide judiciaire.

De nombreux États incitent leurs points de contact à promouvoir leur rôle parmi les autorités nationales et/ou leurs homologues étrangères (Belgique, Bulgarie, Croatie, Danemark, Espagne, États-Unis, France, Hongrie, Italie, Japon, Lituanie, Malte, Maurice, Moldova, Pays-Bas, République dominicaine, Roumanie, Serbie, Slovaquie, Suisse, Turquie).

Certains États veillent à ce que leurs agents enseignent ou participent à des réunions et des formations concernant le réseau 24/7, tant au niveau national qu'avec des partenaires étrangers (Belgique, Croatie, Espagne, États-Unis, Hongrie, Italie, Lettonie, Liechtenstein, Maurice, Moldova, Roumanie, Turquie).

Dans quelques États, les autorités compétentes et les points de contact 24/7 travaillent ou participent à des procédures de suivi pour superviser le traitement des demandes basées sur l'article 31 et faire un retour d'information à l'État requérant (Espagne, États-Unis, Hongrie, Lituanie, Malte, Slovaquie, Turquie).

Un nombre important ont formellement ou effectivement créé des points de contact dans les services de poursuite (Albanie, Belgique, Espagne, États-Unis, France, Italie, Liechtenstein, Lituanie, Malte, Maurice, Pays-Bas, Roumanie, Serbie, Slovaquie, Suisse, Turquie). Moldova et la Pologne envisagent de le faire.

De même, dans un nombre important d'États, les points de contact 24/7 facilitent ou soutiennent le traitement des demandes « article 31 » (Arménie, Australie, Bulgarie, Canada, Danemark,

[11] Il est parfois difficile de déterminer, au vu de réponses assez brèves, quelles mesures ont été prises par un pays ou sur quel élément de la question portent les réponses. Les États souhaiteront peut-être compléter ou modifier la description de leurs mesures.
L'Allemagne, Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question.

Espagne, États-Unis, France, Liechtenstein, Lituanie, Malte, Maurice, République tchèque, Roumanie, Serbie, Slovaquie, Suisse, Turquie).

2.5.2 Exemples de bonnes pratiques

Bulgarie : le point de contact se réunit très fréquemment avec différents organes d'application de la loi en Bulgarie pour promouvoir son rôle et ses capacités. Il est situé à l'intérieur de l'unité d'enquête sur la cybercriminalité de la Direction générale de lutte contre le crime organisé, afin d'assurer qu'il dispose d'un personnel convenablement formé et de responsabilité et capacités nationales. Il entretient, à travers un réseau de connexions informelles, de bonnes relations avec différentes organisations gouvernementales et non gouvernementales et le secteur privé.

France : les policiers extrêmement formés qui sont affectés au point de contact 24/7 font partie de la brigade française spécialisée dans les enquêtes sur la cybercriminalité, ce qui facilite l'échange d'expériences concrètes. Le point de contact 24/7 est en contact direct avec l'autorité centrale pour assurer le meilleur traitement des requêtes de cyber-coopération judiciaire. Il informe ses homologues étrangers des éléments à inclure dans une demande d'entraide judiciaire et, le cas échéant, les met en relation avec l'autorité centrale.

Lituanie : le point de contact 24/7 est l'unité spécialisée de lutte contre la cybercriminalité du Bureau de la police criminelle et sert également de point de contact avec Europol, les prestataires de services et les bureaux des procureurs. Il informe les autres personnels concernés de ses activités au moyen de sessions de formation et de réunions. Il assiste fréquemment les États requérants, les unités de la police nationale et les autorités de poursuite en cas de requêtes « article 31 » et d'autres demandes d'information.

Roumanie : le point de contact est l'unité spécialisée de lutte contre la cybercriminalité du Bureau du Procureur général (Direction des enquêtes sur le crime organisé et le terrorisme, Service de lutte contre la cybercriminalité). Cette unité est légalement chargée de fonctions détaillées telles que : fournir une aide et des informations spécialisées sur la législation, ordonner la préservation immédiate de données informatiques, saisir des objets contenant des données informatiques ou des informations relatives au transfert de données à la demande d'une autorité étrangère compétente. Elle facilite également l'exécution des lettres rogatoires dans les affaires de cybercriminalité. Un point de contact 24/7 secondaire a été créé au sein de la police nationale roumaine pour aider le point de contact existant au sein du Bureau du Procureur général, à savoir le Service de lutte contre la cybercriminalité. Les deux points de contact coordonnent étroitement leurs activités.

États-Unis : le personnel du point de contact 24/7, la Division pénale du Département de la Justice chargée de la lutte contre la cybercriminalité et le vol de propriété intellectuelle, est spécialisé dans la lutte contre la cybercriminalité et le vol de propriété intellectuelle, la collecte de preuves électroniques et la coopération internationale. Le personnel de l'autorité centrale est formé à la cyber-coopération judiciaire. Le CCIPS et l'autorité centrale travaillent ensemble en permanence. Ces bureaux dirigent ou participent tous les ans à de nombreuses activités de formation à l'intention de leurs collègues nationaux et étrangers et encouragent fortement la participation au réseau 24/7. Lors de ces activités et d'autres, les États-Unis s'efforcent d'obtenir un retour d'information sur leurs processus d'entraide judiciaire.

2.5.3 Conclusion

Les États ont adopté diverses mesures pour renforcer les liens entre les unités chargées de traiter les demandes de cyber-coopération judiciaire. Ces mesures sont décrites en détail dans la

synthèse des réponses des Parties, qui est à la disposition de toutes les Parties. Le T-CY recommande de continuer à mettre l'accent sur l'amélioration du processus. Le Conseil de l'Europe devrait soutenir – y compris au moyen de projets – le partage d'expériences entre les points de contact 24/7.

2.6 Rec 6 – Rationalisation des procédures d'entraide judiciaire

> Les Parties devraient considérer la rationalisation des procédures et réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. À cet égard, les Parties doivent partager les bonnes pratiques avec le T-CY.

2.6.1 Aperçu général des suites données à la Recommandation

En formulant cette Recommandation, les Parties ont exprimé la conviction que les États peuvent prendre des mesures internes à l'échelon national pour simplifier leurs procédures d'entraide judiciaire, sans attendre que de tels changements soient exigés par un traité. Les États sont en mesure d'identifier les étapes internes qui ne sont plus nécessaires, en particulier à l'ère numérique.

La plupart des États déclarent avoir déjà rationnalisé leurs procédures[12]. Lorsqu'ils fournissent des précisions au sujet des mesures adoptées à cet égard, les États mentionnent généralement : le traitement rapide des demandes de cyber-coopération judiciaire, l'autorisation des contacts directs de procureur à procureur ou de juge à juge, les consultations (par exemple, avec l'autorité requérante ou le bureau chargé de l'exécution de la requête) et/ou l'utilisation de moyens de communication électroniques (Australie, Espagne, Estonie, Hongrie, Japon, Liechtenstein, Lituanie, Malte, Maurice, Norvège, République tchèque, Roumanie, Serbie, Slovaquie, Slovénie).

Le Danemark et la France mentionnent différentes procédures concernant les États membres de l'Union européenne. Lorsque cela est autorisé par le traité applicable, les demandes d'entraide judiciaire urgentes sont envoyées directement à l'autorité judiciaire compétente.

L'Italie et les Pays-Bas étudient les moyens d'améliorer leurs systèmes et prévoient d'introduire une législation à ce sujet.

2.6.2 Exemples de bonnes pratiques

Autriche : des informations sur les bonnes pratiques classées par pays sont disponibles via intranet.

Azerbaïdjan : la réglementation interne a été modifiée par le Bureau du Procureur général afin que des procureurs puissent exécuter les requêtes urgentes et importantes.

Belgique : les mesures de perquisition et de saisie en relation avec une requête d'entraide judiciaire devaient auparavant être autorisées deux fois : une première fois avant leur exécution et une seconde fois avant la transmission des preuves. Cette double autorisation a été supprimée.

République tchèque : lorsque des points de contact directs entre procureurs ou juges ont été établis par traité, les procureurs ou les juges concernés sont responsables de l'affaire et des communications mais les deux autorités judiciaires centrales pour l'entraide judiciaire peuvent jouer un rôle de soutien. Les bureaux des procureurs des échelons inférieurs ne communiquent normalement qu'avec le bureau immédiatement supérieur ; cependant, dans les affaires d'entraide judiciaire, les procureurs de tous les échelons peuvent contacter directement l'autorité centrale13. Le ministère de la Justice est en contact direct avec tous les juges tchèques.

[12] L'Allemagne, Chypre, la Croatie, la Finlande, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. L'Albanie, la Bulgarie, Israël, le Portugal et la Suisse ont indiqué n'avoir aucun développement nouveau à rapporter en ce domaine.

[13] Ce mécanisme s'applique lorsqu'un traité ne prévoit pas de contacts directs.

États-Unis : l'autorité centrale a créé une cyber-unité pour s'occuper de la cyber-coopération judiciaire. Lorsque cela est possible, cette unité exécute les requêtes elle-même sans la référer à un bureau du procureur fédéral à l'intérieur des États-Unis. Les procureurs de la cyber-unité sont responsables d'États ou de régions spécifiques. De cette façon, les homologues étrangers disposent d'un point de contact connu et constant auquel ils peuvent transmettre leurs questions et leurs requêtes.

2.6.3 Conclusion

La plupart des États semblent considérer qu'ils ont fait tout ce qui leur était possible ; quelques États indiquent de nouvelles mesures concrètes. Le T-CY recommande aux États de continuer à examiner les étapes qui pourraient être supprimés, en particulier au vu des mesures prises par les États partenaires.

2.7 Rec 7 – Utilisation de tous les canaux disponibles

> 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.

2.7.1 Aperçu général des suites données à la Recommandation

Cette Recommandation était motivée par le fait que, premièrement, les canaux d'entraide judiciaire formels sont généralement trop lents et qu'une autre méthode légalement appropriée pourrait être plus rapide ; et, deuxièmement, que les canaux d'entraide judiciaire formels sont de plus en plus (au moins dans certains États) congestionnés par le nombre, qui augmente énormément, de demandes de preuves électroniques. D'autres modalités légalement appropriées de transfert de preuves en dehors des canaux formels non seulement permettraient de gagner du temps, mais faciliteraient également le traitement des requêtes qui doivent obligatoirement passer par les canaux formels.

La plupart des États utilisent tous les canaux pertinents, y compris le réseau 24/7, les canaux de police à police, les agents de liaison étrangers, Europol, la voie diplomatique, Interpol, l'Association internationale des procureurs, Eurojust, le Réseau judiciaire européen, d'autres réseaux de coopération et l'entraide judiciaire formelle[14]. Certaines réponses sont plus nuancées ; plusieurs États indiquent qu'ils peuvent choisir un canal différent si les circonstances l'exigent (Azerbaïdjan, Croatie, Monténégro).

Deux États déclarent spécifiquement avoir adressé directement des demandes à des fournisseurs de services internet (FSI) basés aux États-Unis sans faire appel aux autorités américaines, comme l'autorise la législation des États-Unis (Bulgarie, Lituanie). Cependant, d'autres sources – par exemple, les rapports de transparence des FSI – indiquent que d'autres États que la Bulgarie et la Lituanie envoient directement des demandes à des FSI basés aux États-Unis. Il semble donc que plusieurs États aient omis ce fait dans leurs réponses (de nombreux États semblent aussi avoir répondu à la question 7 seulement en tant qu'État requis et non en tant qu'État requérant).

2.7.2 Exemples de bonnes pratiques

Canada : le Canada encourage l'utilisation de tous les canaux disponibles, y compris l'entraide judiciaire formelle, la coopération de police à police et la coopération entre autorités de poursuite. Son autorité centrale a établi une liste de ses homologues étrangers indiquant les types de preuves pouvant être obtenus sans avoir à passer par l'entraide judiciaire formelle. Dans ses activités de formation de partenaires étrangers, le Canada attire régulièrement l'attention sur l'aide pouvant être obtenue en dehors de l'entraide judiciaire.

Israël : Israël a créé un « Cyber-centre national » au sein de l'Unité de lutte contre la cybercriminalité de la police et un Service de lutte contre la cybercriminalité au sein du Bureau du Procureur général. Ces services facilitent le traitement des demandes via des canaux non formels.

Italie : la police judiciaire facilite la coopération de police à police et traite les requêtes d'entraide judiciaire. Un protocole de communication efficace permet d'harmoniser et d'accélérer les pratiques de la police et des bureaux des procureurs.

[14] L'Allemagne, Chypre, la Finlande, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. L'Albanie a indiqué n'avoir aucun développement nouveau à rapporter en ce domaine.

2.7.3 Conclusion

La plupart des États affirment utiliser tous les canaux disponibles pour obtenir des informations et mettre de nombreux canaux à la disposition des États qui cherchent à obtenir d'eux des informations. Le T-CY recommande de développer et d'utiliser le plus possible, dans les limites définies par la législation pertinente, des canaux informels. Cela permettra d'accélérer l'aide et de réduire l'arriéré des demandes dans les canaux formels.

2.8 Rec 8 – Procédures d'urgence

> 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 services.

2.8.1 Aperçu général des suites données à la Recommandation

Quelques États ont établi des procédures d'urgence formelles ; cette Recommandation visait à connaître les procédures suivies par les autres États.

Un nombre réduit d'États ont répondu en détail à cette question15. La plupart se contentent d'indiquer comment ils reçoivent et traitent les requêtes urgentes mais ne précisent pas s'il existe des pouvoirs juridiques spéciaux permettant de fournir des preuves plus rapidement. La plupart des États n'évoquent pas spécifiquement les situations où une vie est en danger.

Presque toutes les réponses reconnaissent que des situations d'urgence peuvent se produire eu égard à l'obtention de preuves électroniques. Presque tous les États déclarent que, dans une situation d'urgence, leurs agents travaillent plus et plus rapidement et signalent à leurs collègues nationaux qu'une affaire est urgente. Ces pratiques ne doivent pas être sous-estimées et leurs résultats doivent être reconnus avec gratitude. Cependant, elles dépendent de la diligence et de la motivation des agents concernés et non d'une procédure établie et bien comprise[16].

Aucun État n'a mis en place une procédure d'urgence entièrement fiable couvrant toutes les catégories de données y compris les données sur le contenu. La législation des États-Unis autorise la divulgation des données relatives aux abonnés, des données de trafic et des données sur le contenu dans les situations d'urgence mais l'application de cette disposition n'est pas obligatoire. Les fournisseurs de services internet qui sont soumis au droit américain ont donc toute discrétion d'accepter ou de refuser la divulgation des données.

2.8.2 Exemples de bonnes pratiques

Plusieurs États déclarent prendre note en général de l'urgence d'une requête. Il arrive aussi qu'ils prennent conscience de l'urgence d'une requête alors que l'État requérant ne l'a pas signalé. Ils s'efforcent ensuite de traiter la requête le plus rapidement possible (Arménie, Canada, Danemark, Estonie, États-Unis [lorsque la divulgation volontaire n'est pas applicable], Israël, Italie, Liechtenstein, Serbie, Turquie).

Bulgarie : lorsque l'État requérant indique qu'une requête est urgente, des procédures au titre de la Loi sur les communications électroniques permettent l'accès rapide aux données demandées.

Lettonie : en vertu de la réglementation, une affaire est présumée urgente dès lors qu'elle implique la prévention ou la divulgation d'une infraction pénale, la protection de la vie d'un individu et la protection de l'État ou de la sécurité publique. En pareils cas, plusieurs catégories de données relatives aux abonnés peuvent être divulguées dans un délai de trois heures ou même parfois plus rapidement.

Suisse : les autorités de poursuite peuvent décider au cas par cas de passer outre ou de reporter certains éléments de procédure ou conditions préalables qui pourraient ralentir le processus.

---

[15] Chypre, la Croatie, la Finlande, la Géorgie, la Hongrie, l'Islande, le Japon, la Lituanie, le Luxembourg, Moldova, les Pays-Bas, le Panama, le Portugal, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, la Slovaquie, la Slovénie, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. L'Albanie, l'Australie, l'Autriche, la France, Maurice, le Monténégro et la Roumanie ont renvoyé à leurs réponses précédentes ou n'avaient aucun développement nouveau à signaler.

[16] L'Allemagne examine actuellement l'ordonnance relative aux procédures d'urgence.

2.8.3 Conclusion

Le nombre d'affaires dans lesquelles des vies sont en danger ou qui présentent un risque de blessures physiques, et pour lesquelles l'obtention de preuves électroniques conservées à l'étranger est décisive, augmente et il est plus que probablement que cette tendance ne va pas s'inverser. Sans doute parce que les décideurs ne sont pas conscients des efforts frénétiques que déploient les agents chargés de la lutte contre la cybercriminalité pour s'entraider dans les situations d'urgence, les États n'ont guère développé – ou pas du tout – de procédures numériques spécifiques d'urgence et se fient à leur personnel spécialisé pour trouver une solution dans les situations d'urgence. Le T-CY recommande de fournir aux décideurs des informations sur cette question et de poursuivre les efforts engagés au niveau national pour améliorer et formaliser les dispositifs d'urgence.

2.9 Rec 9 – Accusé réception des demandes et notification des mesures prises

> Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.

2.9.1 Aperçu général des suites données à la Recommandation

Cette Recommandation a été adoptée en réponse aux déclarations des Parties selon lesquelles il est fréquent pour elles de ne pas savoir si une requête d'entraide judiciaire a été reçue, si son traitement progresse et à qui adresser les questions. Cela est particulièrement frustrant dans le cas des requêtes qui sont en instance depuis des mois ou des années.

La plupart des États déclarent confirmer systématiquement, sous une forme ou une autre, la réception des requêtes d'entraide judiciaire. Ils notifient également, de leur propre chef ou sur demande, les États requérants des mesures matérielles prises en relation avec une requête17.

- Plusieurs États (Australie, Estonie, Finlande, Hongrie, Italie, Liechtenstein, Malte, Norvège, Roumanie, Serbie, Slovaquie) accusent systématiquement réception des requêtes d'entraide judiciaire et fournissent aussi de leur propre chef des informations sur les mesures prises suite à la requête et/ou les coordonnées de la personne chargée de traiter l'affaire.

- D'autres accusent systématiquement réception des requêtes mais fournissent uniquement sur demande des informations sur leur traitement et la personne à contacter (États-Unis, Slovénie).

- Un groupe important d'États accusent réception des requêtes sur demande (Arménie, Autriche, Azerbaïdjan, Belgique, Bosnie et Herzégovine, Canada, Espagne, Japon, Lettonie, Moldova, Monténégro, République dominicaine, Turquie). Certains d'entre eux fournissent aussi des informations sur le traitement des requêtes.

Deux États – la Bulgarie et la Suisse – n'ont pas mis en place de procédures pour accuser réception des requêtes. Cependant, la Bulgarie y travaille actuellement.

Plusieurs Parties (Azerbaïdjan, France, Israël, Lituanie, Maurice, Pays-Bas) déclarent que les points de contact 24/7 accusent réception des demandes. Certains fournissent systématiquement ou sur demande des informations sur les mesures prises. Cependant, dans les réponses de ces États, il n'apparaît pas clairement si cela s'applique aux requêtes d'entraide judiciaire ou seulement aux demandes initiales 24/7.

Au niveau de l'UE[18], par exemple, les États membres doivent veiller à mettre en place des procédures afin que, s'agissant des demandes d'aide urgentes, l'autorité compétente puisse indiquer, dans les huit heures suivant la réception, au minimum s'il sera répondu à la demande, ainsi que les modalités et le délai estimé pour cette réponse.

[17] L'Allemagne, Chypre, la Croatie, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. L'Albanie et le Portugal ont indiqué n'avoir aucun développement à rapporter en ce domaine.

[18] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la Décision-cadre du Conseil 2005/222/JAI.

2.9.2 Exemples de bonnes pratiques

Australie : l'autorité centrale accuse réception par écrit (normalement par courriel) des requêtes qu'elle reçoit dans un délai de deux à cinq jours ouvrables, en leur attachant un numéro de dossier. Une fois qu'une requête est confiée à un agent de l'autorité centrale, celui-ci envoie ses coordonnées au requérant étranger pour faciliter la communication d'information.

Hongrie : la Hongrie accuse réception des requêtes dans tous les cas et communique au pays requérant des informations sur les principales mesures prises pour les mettre en œuvre. Elle notifie également par écrit la Partie requérante lorsque la requête est transmise au bureau du procureur pertinent (en indiquant ses coordonnées).

Liechtenstein : lorsqu'une requête est confiée à un juge, un accusé de réception est immédiatement envoyé à l'État requérant, avec un numéro de dossier et les coordonnées du juge. L'État requérant est informé du traitement de l'affaire et reçoit ensuite les preuves demandées ou bien les motifs de refus de la requête.

2.9.3 Conclusion

La meilleure pratique est d'accuser systématiquement réception des requêtes et, dans la suite de la procédure, de communiquer systématiquement les coordonnées des personnes chargées de les traiter, ainsi que des mises à jour sur l'avancement de la procédure. Cependant, les États ne disposent pas toujours de ressources suffisantes pour le faire. Le T-CY recommande, par conséquent, que le point de réception des requêtes d'entraide judiciaire – y compris s'il s'agit d'un point de contact 24/7 recevant non seulement des demandes 24/7 mas aussi des requêtes d'entraide judiciaire – en accuse systématiquement réception.

Les États ont fourni des réponses très diverses et n'indiquent pas toujours clairement s'il est facile en pratique d'obtenir des informations sur la personne à contacter et l'état d'avancement du dossier. Le T-CY souligne, par conséquent, que les États devraient prendre toutes les mesures possibles pour huiler le mécanisme. Un État requis doit faire en sorte que l'État requérant sache effectivement à qui adresser les demandes d'information sur le traitement de la requête. Ces demandes peuvent être traitées par l'autorité centrale ou un bureau du procureur, par exemple, mais le système ne peut fonctionner si l'État requérant ne sait pas qui contacter. Enfin, au fur et à mesure de la procédure, les agents pertinents de l'État doivent fournir rapidement des informations sur le traitement de la requête.

2.10 Rec 10 – Ouverture d'enquêtes nationales

> Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide judiciaire.

2.10.1 Aperçu général des suites données à la Recommandation

Le point essentiel de cette Recommandation est que le transfert d'information par les États devrait être rendu aussi facile que le permet la législation. La Convention de Budapest fournit à l'article 26 une base juridique au transfert d'information spontanée puisque cette information peut aider un autre État à poursuivre la criminalité. De la même façon, les preuves obtenues dans le cadre d'une enquête nationale peuvent faciliter une enquête menée par un autre État.

La question relative à cette Recommandation était une question composite et, dans bien des cas, les États n'ont répondu qu'à certaines parties de cette question[19].

- De nombreux États déclarent qu'ils peuvent utiliser l'information spontanée qui leur est envoyée (Arménie, Australie, Azerbaïdjan, Belgique, Canada, Danemark, Lettonie, Maurice, Norvège, Portugal, République tchèque, Roumanie, Serbie).

- Un petit groupe d'États déclarent spécifiquement qu'ils peuvent transmettre l'information spontanée à d'autres États (Croatie, Liechtenstein, République tchèque, Roumanie, Suisse, Turquie).

- D'une manière générale, les États peuvent envisager d'ouvrir – ou sont tenus d'ouvrir – une enquête nationale sur demande étrangère. Une procédure n'est ouverte que si les conditions nationales sont satisfaites et que cela semble approprié (Albanie, Allemagne, Arménie, Australie, Autriche, Belgique, Bosnie et Herzégovine, Canada, Danemark, Espagne, États-Unis, Finlande, France, Japon, Liechtenstein, Maurice, Pologne, Portugal, République tchèque, Roumanie, Serbie, Slovaquie)20.

- Quelques États n'ouvrent pas normalement une enquête nationale sur demande étrangère (Lituanie, Moldova, Monténégro). La Lituanie indique que cela ne restreint aucunement le partage d'information, ni ne ralentit l'entraide judiciaire car l'initiation d'une enquête nationale n'est pas nécessaire pour accélérer le processus d'obtention de preuves. Moldova a ouvert une procédure de ce type impliquant des preuves électroniques.

2.10.2 Exemples de bonnes pratiques

Autriche : l'ouverture d'une enquête nationale sur demande étrangère est fréquente.

Danemark : l'autorité chargée de traiter la requête d'entraide judiciaire examine dans tous les cas la possibilité [d'initier une procédure nationale].

[19] Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. La Bulgarie et Israël ont indiqué n'avoir aucun développement à rapporter en ce domaine.

[20] Au Portugal, une enquête nationale peut être ouverte à des fins nationales, non pour aider la coopération internationale. La Roumanie et la Slovaquie indiquent que l'information contenue dans une requête d'entraide judiciaire ne peut être utilisée qu'à des fins limitées. Par conséquent, il est parfois nécessaire d'obtenir une autorisation avant d'utiliser cette information pour ouvrir une enquête nationale.

Liechtenstein : lorsqu'une requête d'entraide judiciaire contient des informations relevant de l'autorité pénale nationale, une procédure pénale doit être ouverte, ce qui se produit régulièrement.

Norvège : une enquête nationale peut être ouverte lorsqu'il existe un lien entre les faits matériels de l'affaire et la Norvège. Il n'est pas nécessaire qu'un autre État le demande à la Norvège ; les autorités norvégiennes examinent elles-mêmes cette possibilité.

Serbie : une enquête nationale est ouverte sur demande et toute l'information pertinente recueillie dans la procédure est partagée avec les autorités étrangères.

2.10.3 Conclusion

Les enquêtes électroniques requièrent de plus en plus fréquemment la participation de plusieurs pays. Une affaire peut englober des activités ou des victimes disséminées dans une dizaine ou une vingtaine d'États et, d'un point de vue pratique, les enquêteurs d'un pays peuvent réduire très fortement le travail des enquêteurs d'autres pays en partageant leurs données. Les réponses recueillies dans cette enquête ne permettent pas d'établir avec quelle fréquence la fourniture spontanée d'information ou l'ouverture d'une procédure pénale ont lieu et si ces pratiques facilitent par conséquent l'aide autant qu'elles le pourraient.

2.11 Rec 11 – Transmission électronique des demandes

> Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.

2.11.1 Aperçu général des suites données à la Recommandation

Cette Recommandation répond à la nécessité de rationaliser le processus de l'entraide judiciaire de toutes les façons possibles.

Les réponses peuvent être réparties en deux groupes. Les répondants ont indiqué en général : 1) s'ils envoient des demandes par la voie électronique, ou 2) s'ils autorisent d'autres États à le faire. Peu d'États ont répondu aux deux volets de la question[21].

Dans de nombreux États, la transmission électronique est autorisée dans le cas des affaires urgentes, lorsqu'un État partenaire en fait la demande ou à condition que la demande électronique soit suivie par une demande sur papier (Azerbaïdjan, Belgique, Bosnie et Herzégovine, Bulgarie, Croatie, États-Unis, Japon, Liechtenstein, Lituanie, Monténégro, Pologne, République tchèque, Slovaquie, Suisse). Le Canada encourage la soumission électronique des demandes.

Certains États déclarent que la transmission électronique est possible ou fréquemment utilisée mais sans préciser si elle est utilisée à la fois pour les demandes reçues et envoyées et dans les cas non urgents (Albanie, Arménie, Australie, Autriche (« souvent utilisée »), Espagne, Estonie, Finlande, France, Hongrie, Malte, Norvège, Pays-Bas, Roumanie, Serbie).

2.11.2 Exemples de bonnes pratiques

Hongrie : les canaux de communication électronique comme le réseau SIENA d'Europol, Interpol ou le courrier électronique sont utilisés de préférence.

Malte : la télécopie, le courrier électronique et la copie papier sont utilisés.

Pays-Bas : la télécopie et le courrier électronique sont couramment utilisés.

Norvège : la pratique actuelle est l'utilisation du courrier électronique.

Serbie : les demandes reçues et envoyées sont transmises par courrier électronique suivi d'une demande sur papier.

Espagne : la télécopie et le courrier électronique sont couramment utilisés.

2.11.3 Conclusion

On voit mal pourquoi la transmission électronique des demandes ne pourrait être autorisée dans tous les cas, pas seulement dans les affaires urgentes (même si l'envoi d'une demande papier est exigé ensuite). Aucun pays n'invoque la sécurité électronique comme raison d'interdire la transmission électronique des demandes. Il se peut simplement que les États ne soient pas encore habitués aux demandes sous forme électronique. Les États doivent réaliser, cependant, qu'avec l'augmentation du nombre des demandes, l'utilisation du papier cessera d'être pratique.

[21] L'Allemagne, Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. L'Italie a indiqué n'avoir aucune information nouvelle à fournir à ce sujet. Dans certains cas, en outre, il n'apparaît pas clairement si la réponse du pays porte sur les demandes 24/7 ou sur les demandes d'entraide judiciaire ; ces réponses, par conséquent, ne sont pas résumées ici.

2.12 Rec 12 – Demandes spécifiques contenant toutes les informations nécessaires

> Les Parties veillent à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.

2.12.1 Aperçu général des suites données à la Recommandation

Les États se plaignent fréquemment de l'omission d'éléments très importants – des faits matériels aux coordonnées de l'organe requérant – dans les requêtes d'entraide judiciaire et des retards inutiles qui en résultent.

La plupart des États affirment qu'ils veillent déjà à ce que leurs demandes soient spécifiques et contiennent toutes les informations nécessaires (Albanie, Australie, Autriche, Azerbaïdjan, Belgique, Bosnie et Herzégovine, Canada, Croatie, Danemark, Espagne, Estonie, États-Unis, Finlande, France, Hongrie, Japon, Lettonie, Liechtenstein, Lituanie, Malte, Maurice, Moldova, Monténégro, Pays-Bas, Portugal, République tchèque, Roumanie, Serbie, Slovaquie, Slovénie, Suisse, Turquie)22.

Plusieurs États indiquent spécifiquement que leur autorité centrale examine les requêtes avant envoi pour vérifier qu'elles sont complètes. Lorsqu'une requête doit être améliorée avant envoi, l'autorité centrale en discute avec les rédacteurs concernés (Australie, Espagne, États-Unis, France, Japon, Malte, Moldova, République tchèque, Roumanie, Serbie, Slovaquie, Turquie).

Les États mentionnent également à ce propos :

- l'organisation de formations à l'intention des différentes catégories d'agents publics chargés de préparer les requêtes d'entraide judiciaire (Belgique, Maurice, Monténégro, Pays-Bas, Slovaquie);
- l'existence de modèles, listes de contrôle, guides ou normes légales s'appliquant aux requêtes (Australie, Belgique, Croatie, Danemark, France, Lettonie, Maurice, Moldova, Pays-Bas, République tchèque, Serbie, Slovaquie) ;
- le travail de consultation et de liaison avec l'État requis (Canada, Estonie, États-Unis, France, Lituanie, Malte).

2.12.2 Exemples de bonnes pratiques

Australie : l'autorité centrale utilise, pour les demandes envoyées à l'étranger, un formulaire standard qui inclut les différentes catégories d'information exigées par ses partenaires. L'autorité centrale est prête à recevoir un retour d'information sur les points spécifiques à inclure dans les requêtes envoyées par l'Australie.

France : l'autorité centrale et les magistrats qui jouent un rôle de liaison en dehors de la France examinent les requêtes d'entraide judiciaire, y compris au moyen de consultations. La France a également produit un guide portant spécifiquement sur l'obtention de données électroniques conservées aux États Unis.

Maurice : les demandes doivent être conformes aux formats présentés dans les formations GLACY et aux normes légales mauriciennes.

[22] L'Allemagne, Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. La Bulgarie et la Norvège ont indiqué n'avoir aucune information nouvelle à fournir à ce sujet.

Moldova : les demandes doivent inclure les éléments spécifiques énumérés dans le code de procédure pénale.

Monténégro : le centre national de formation des juges et des procureurs organise régulièrement des formations consacrées à l'entraide judiciaire à l'intention des juges et des procureurs. De plus, au moins une fois par an, le ministère de la Justice organise des réunions régionales, avec des représentants des ministères de la Justice et du système judiciaire des États avec lesquels il a conclu des accords bilatéraux, en vue d'accroître l'efficience de l'entraide judiciaire.

Slovaquie : les procureurs slovaques ont pu suivre de nombreuses sessions de formation sur l'obtention de preuves d'un pays étranger et, en particulier, des États-Unis. Il existe, à tous les niveaux du système (districts, régions, centre), des procureurs spécialisés dans la coopération internationale. Le Bureau de Procureur général leur fournit des directives. Certains de ces procureurs ont été formés conjointement avec les experts de l'Unité de lutte contre la cybercriminalité de la Direction de la police. Des activités de formation concernant les requêtes d'entraide judiciaire et, en particulier, les demandes de preuves électroniques ont également été organisées par l'Académie judiciaire à l'intention des juges et des procureurs.

2.12.3 Conclusion

D'une manière générale, les États semblent prêter une forte attention au problème des requêtes d'entraide judiciaire inadéquates. Néanmoins, les États requis continuent à se plaindre des lacunes des requêtes qu'ils reçoivent. Les différentes méthodes décrites ci-dessus pour remédier à ces imperfections – examen par l'autorité centrale, formation, listes de contrôle, spécialisation, consultations – devraient permettre d'améliorer assez rapidement le processus de rédaction, si elles sont appliquées avec le sérieux suffisant. Certains problèmes relatifs aux preuves électroniques sont très difficiles à résoudre ; cependant, des efforts raisonnables devraient conduire à une amélioration des requêtes.

2.13 Rec 13 – Flexibilité dans l'application des normes de double incrimination

> Conformément à l'article 25.5 de la 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 pour faciliter l'octroi de l'aide.

2.13.1 Aperçu général des suites données à la Recommandation

L'obtention de preuves électroniques est devenue importante dans la répression de toute une gamme d'infractions pénales pour lesquelles l'aide internationale était auparavant inutile. Cette Recommandation appelle instamment les Parties à faire en sorte que les critères juridiques requis pour la transmission de preuves puissent être interprétés de manière à fournir l'aide la plus étendue possible.

La plupart des États s'efforcent de faire preuve de flexibilité dans l'application de la double incrimination, en s'appuyant sur la Convention de Budapest et en prenant en considération les faits de l'infraction alléguée plutôt que son classement dans une catégorie d'infractions ou la terminologie employée au sens strict pour la désigner (Albanie, Arménie, Australie, Autriche, Azerbaïdjan, Belgique, Bosnie et Herzégovine, Canada, Croatie, Espagne, Estonie, États-Unis, Finlande, France, Japon, Lituanie, Malte, Maurice, Portugal, République tchèque, Roumanie, Serbie, Suisse)[23].

Plusieurs États déclarent n'avoir encore rencontré aucun cas où la double incrimination aurait justifié le refus d'octroyer l'aide judiciaire ou affirment que, bien que n'ayant pas encore rencontré le problème à ce jour, ils feraient preuve de flexibilité dans le cas où celui-ci se présentait (Albanie, Italie, Monténégro, Slovaquie).

D'autres États considèrent que le critère de double incrimination doit être respecté lorsque l'application de mesures coercitives telles que perquisition, saisie ou interception et enregistrement de télécommunications est requise (Belgique, Danemark, Norvège, Pays-Bas, République tchèque, Turquie). Pour apporter l'aide demandée, ces États peuvent, par exemple, chercher à obtenir des éléments supplémentaires du pays requérant ou offrir une forme d'aide non soumise au critère de double incrimination.

Deux États déclarent ne pouvoir faire preuve de flexibilité dans l'application de la double incrimination (Liechtenstein, Pologne).

2.13.2 Exemples de bonnes pratiques

Canada : sauf quelques exceptions, la législation canadienne n'exige pas la double incrimination. Dans les cas bien délimités où son application est requise, le Canada fait preuve de flexibilité en se basant sur la conduite en cause, sans exiger la présence dans le droit canadien d'un équivalent exact à l'infraction étrangère.

Portugal : les autorités portugaises apportent leur coopération, même sans réciprocité, en se fondant sur la nature des faits ou sur la nécessite de combattre certaines formes de criminalité graves. Elles peuvent également le faire dans les cas où la coopération peut contribuer à améliorer la situation de l'accusé ou sa réinsertion sociale, ou à clarifier des faits se rapportant à un ressortissant portugais.

[23] L'Allemagne, Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, la Slovénie, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. La Bulgarie a indiqué n'avoir aucun développement nouveau à rapporter en ce domaine.

Serbie : la norme de double incrimination est appliquée de manière flexible, afin de faciliter l'octroi de l'aide. Si l'infraction pénale faisant l'objet d'une requête d'entraide judiciaire n'est pas réprimée dans le droit pénal serbe, la Serbie s'efforce, dans la mesure du possible, d'appliquer les dispositions de son code pénal visant des éléments et un mode opératoire se rapprochant le plus de l'acte décrit dans la requête.

2.13.3 Conclusion

Les États déclarent qu'ils font de leur mieux pour agir avec flexibilité et s'apporter mutuellement une aide sur la base de la législation nationale et des accords internationaux. Néanmoins, certains d'entre eux devraient réfléchir à la possibilité de faire preuve d'une plus grande flexibilité, comme les y encourage la Convention de Budapest.

2.14 Rec 14 – Consultation préalable

> Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.

2.14.1 Aperçu général des suites données à la Recommandation

Cette Recommandation visait à répondre aux réclamations des Parties selon lesquelles les requêtes formelles d'entraide judiciaire imparfaites font perdre du temps à la fois à l'État requérant et à l'État requis et n'aboutissent pas au transfert de preuves. Les Parties ont souligné que des contacts très simples (appel téléphonique, courrier électronique) à un stade précoce du processus permettent de résoudre des erreurs ou des problèmes avant de consacrer du temps à une requête formelle insuffisante.

La plupart des Parties consultent l'État requis avant d'envoyer une requête formelle d'entraide judiciaire. Cette consultation préalable prend des formes diverses : envoi de questions par courrier électronique, transmission du projet de requête pour obtenir les commentaires de la Partie requise, ou envoi de questions à un agent de liaison étranger présent dans le pays. Certains États ne consultent normalement au préalable l'État requis que dans le cas d'une affaire sensible ou complexe ou lorsque cet État est un partenaire nouveau[24].

Quelques États ne semblent pas consulter normalement l'État requis avant d'envoyer la requête (Moldova, Turquie).

2.14.2 Exemples de bonnes pratiques

Bulgarie : lorsque cela est possible, les organes de répression bulgares consultent activement les autorités de la Partie requise avant d'envoyer une requête. Ils coopèrent, par exemple, avec les autorités des États-Unis par l'intermédiaire des agents de liaison américains présents en Bulgarie et d'autres contacts spécialement désignés en matière de cybercriminalité.

République tchèque : l'autorité centrale et les autorités judiciaires tchèques consultent régulièrement leurs partenaires étrangers les plus fréquents. Dans les affaires complexes, cette consultation a lieu par écrit directement entre autorités responsables, par l'intermédiaire des réseaux de spécialistes de l'entraide judiciaire ou de réunions de coordination bilatérales ou multilatérales.

France : l'autorité centrale et les magistrats remplissant des fonctions de liaison engagent un dialogue constructif avec les autorités de la Partie requise. La France souligne que ces contacts informels visent à faciliter l'aide et ne doivent pas servir de filtre avant l'envoi d'une requête formelle.

Lituanie : les Parties requises sont généralement consultées avant l'envoi des requêtes, en particulier lorsque la Lituanie travaille avec un nouvel État partenaire ou lorsqu'il s'agit d'une requête sensible ou complexe.

Serbie : si nécessaire, la Serbie consulte préalablement la Partie requise avant de rédiger la requête complète pour assurer que toutes les mesures nécessaires pourront être prises et que toutes les preuves demandées pourront être recueillies.

[24] Plusieurs États approuvent la pratique de consultation préalable mais sans indiquer *s'ils consultent eux-mêmes d'autres États*. Cependant, ils encouragent les autres États à les consulter (Arménie, Australie, Japon, Suisse).

2.14.3 Conclusion

La plupart des Parties déclarent qu'avant d'envoyer une demande formelle d'entraide judiciaire, elles consultent l'État requis, si nécessaire, par l'intermédiaire d'un de plusieurs mécanismes. Ces réponses ne semblent pas cohérentes avec les réclamations qui ont conduit à cette Recommandation. Il se peut que les États recourent maintenant plus fréquemment à des consultations préalables. Quoi qu'il en soit, des consultations préalables plus fréquentes permettront de réduire les erreurs, les dépenses, les retards, la perte de preuves et le travail inutile.

2.15 Rec 15 – Transparence au sujet des conditions applicables, des seuils et des motifs de refus

> 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.

2.15.1 Aperçu général des suites données à la Recommandation

La consultation de sites web pour obtenir des informations essentielles est de plus en plus fréquente. C'est pourquoi les Parties ont suggéré qu'il serait utile, dans la mesure du possible, de publier les conditions applicables sur le web, dans l'intérêt des États requérants. La formation, les consultations, le travail de liaison et d'autres pratiques sont utiles mais elles n'atteignent pas nécessairement toutes les personnes pouvant être impliquées dans la rédaction d'une demande d'entraide judiciaire. Un site web peut atteindre un plus grand nombre de ces agents publics plus rapidement.

De nombreux États n'ont pas répondu à la suggestion de publier l'information essentielle relative à l'entraide judiciaire sur un site web[25]. Ils se contentent de citer ou de fournir des liens aux lois et traités pertinents pour eux et/ou indiquent que les informations concernant chaque affaire, y compris les raisons de refus d'une requête, sont transmises confidentiellement à l'État requérant.

Néanmoins, de nombreux États publient en fait l'information essentielle relative à l'entraide judiciaire et/ou des liens à la législation et aux traités pertinents sur des sites publics ou à accès quelque peu restreint (Australie, Belgique[26], Canada, Espagne, Italie,[27] Japon, Moldova, Pologne, République tchèque, Serbie, Suisse, Turquie). D'autres envisagent de le faire [États-Unis, Finlande, Pays-Bas, République tchèque (publication d'informations plus détaillées qu'actuellement), Slovaquie]. Lorsque cette information n'est publiée que dans la ou les langues nationales, son utilité pour les autres Parties reste limitée.

2.15.2 Exemples de bonnes pratiques

Canada : l'autorité centrale maintient un site web public détaillé qui fournit aux agents publics canadiens et étrangers des informations procédurales et de fond en vue de la rédaction d'une requête d'entraide judiciaire efficace. On trouve aussi sur ce site web des indications sur la manière de requérir une aide sur des questions mineures. Des guides pratiques et des modèles sont accessibles sur le site.

Japon : le site web du ministère de la Justice fournit des explications détaillées en anglais sur les conditions applicables aux demandes d'entraide judiciaire, y compris les motifs de refus.

Moldova : toutes les informations nécessaires sur les conditions applicables aux requêtes d'entraide judiciaire sont publiées sur le site web du Bureau du Procureur général. Ces informations sont actuellement publiées uniquement en moldave mais Moldova envisage de les faire traduire et de les publier également en anglais.

[25] L'Allemagne, Chypre, la Croatie, la Géorgie, la Hongrie, l'Islande, le Luxembourg, le Monténégro, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, la Slovénie, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question. La Bulgarie et Israël ont indiqué n'avoir aucune information nouvelle à fournir à ce sujet.
[26] La Belgique publie cette information sur le site web du PC-OC.
[27] L'Italie utilise le site du Réseau judiciaire européen, qui n'est pas ouvert à toutes les Parties à la Convention de Budapest.

Turquie : l'autorité centrale fournit des informations générales et détaillées au sujet de l'entraide judiciaire sur son site web, qui permet aussi d'accéder à la législation turque régissant les pratiques d'entraide judiciaire.

2.15.3 Conclusion

Plusieurs États ne semblent pas être encore parvenus à héberger et maintenir un site web sur l'entraide judiciaire. Les États qui disposent d'un site à ce sujet devraient publier le plus d'informations générales possibles, notamment à propos de la législation applicable et des traités, ainsi que des modèles de formulaires, des guides et des outils en ligne par exemple, en s'abstenant de publier des informations portant sur des affaires spécifiques. La publication des procédures d'entraide judiciaire permettrait de réduire le volume de travail des agents publics concernés à toutes les étapes du processus de l'entraide judiciaire, aussi bien dans les États requis que dans les États requérants.

3 Période de conservation des données (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 Convention de Budapest. Le T-CY devrait documenter les périodes de conservation.

3.1 Durée de la période de conservation

Le tableau ci-dessous indique la durée des périodes de conservation des données et de leur renouvellement éventuel, telle qu'indiquée par les États :

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période d'extension ou de renouvèlement de la conservation des données spécifiées
Albanie	90 jours	90 jours
Andorre		
Arménie	Pas de limite spécifique.	Aucune information n'a été fournie.
Australie	L'article 3 du chapitre 3-1A de la Loi sur les télécommunications (interception et accès) de 1979 dispose qu'un fournisseur est tenu de conserver les communications depuis le jour où il est notifié d'une demande étrangère jusqu'au jour où la Police fédérale australienne l'informe que cette demande est annulée. La Police fédérale australienne annule une demande de conservation si le pays étranger demandeur ne transmet pas au Procureur général une requête dans un délai de 180 jours.	Il n'existe pas de mécanisme d'extension ou de renouvellement de la période de conservation des données spécifiées. Le pays requérant doit remplir une nouvelle demande de conservation des données. La période effective de conservation de 180 jours excède les 60 jours minimum prévus à l'article 29.
Autriche	La conservation des données n'est pas soumise à une limite spécifique.	L'extension ou le renouvellement sont possibles sur demande de l'État requérant, en prenant en compte la proportionnalité de la mesure de conservation. Il n'est pas prévu de périodes ou de limites spécifiques.
Azerbaïdjan	Aucune information n'a été fournie.	Aucune information n'a été fournie.
Belgique	Aucune information n'a été fournie.	Aucune information n'a été fournie.
Bosnie et Herzégovine	L'harmonisation des dispositions du Règlement sur la conservation des fichiers et documents archivés sera nécessaire pour assurer que la période de conservation de tous les fichiers est conforme à celle prescrite par la Convention. La seule exception concernera les bases de données électroniques de l'autorité centrale qui seront conservées en permanence.	L'harmonisation des dispositions du Règlement sur la conservation des fichiers et documents archivés sera nécessaire pour assurer que la période de conservation de tous les fichiers est conforme à celle prescrite par la Convention. La seule exception concernera les bases de données électroniques de l'autorité centrale qui seront conservées en permanence.

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période d'extension ou de renouvèlement de la conservation des données spécifiées
Bulgarie	3 mois	L'extension de la période de conservation n'est pas autorisée.
Canada	Aux termes de la Loi sur la protection des Canadiens contre la cybercriminalité, le Canada peut conserver des données informatiques à la demande de la police ou sur l'ordre d'un tribunal. Dans un premier temps, la police canadienne adresse normalement une demande de conservation des données au maître du fichier. Le seuil légal requis pour une telle demande est l'existence de soupçons raisonnables que : une infraction réprimée par la législation d'un État étranger a été ou va être commise; une enquête est conduite par une personne ou autorité chargée de l'investigation de ce type d'infraction dans l'État en question ; les données informatiques détenues ou contrôlées par la personne ou l'entité visée par la demande seront utiles pour l'enquête. Les demandes de conservation sont valables pour une durée de 90 jours non renouvelable. Cependant, la police canadienne peut obtenir un ordre de conservation d'un tribunal canadien.	L'extension de la période de conservation n'est pas autorisée.
Croatie	Aucune information n'a été fournie.	Aucune information n'a été fournie.
Chypre		
République tchèque	La législation tchèque ne prévoit pas de limite pour la conservation de données au titre de l'article 29 de la Convention de Budapest. Néanmoins, la requête d'entraide judiciaire doit être envoyée le plus rapidement possible.	
Danemark	6 mois	L'extension de la période de conservation n'est pas autorisée.
République dominicaine	La période prévue est de quatre-vingt-dix (90) jours.	La période de conservation est renouvelable à tout moment sur demande pour un nombre de jours identique.

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période d'extension ou de renouvèlement de la conservation des données spécifiées
Estonie	La conservation des données peut être obtenue très rapidement, si possible pendant une journée.	Les pouvoirs généraux s'appliquent à la conservation des données. La législation ne prévoit pas de conditions ou de périodes supplémentaires.
Finlande	Aucune information n'a été fournie.	Aucune information n'a été fournie.
France	90 jours	90 jours
Géorgie		
Allemagne	Aucune information n'a été fournie.	Aucune information n'a été fournie.
Hongrie	3 mois	Aucune information n'a été fournie.
Islande		
Israël	La législation israélienne autorise la conservation des données pour une période de six mois, sur décision d'un juge.	Un magistrat peut étendre la période de conservation à plus de six mois, sous certaines conditions fixées par lui, en réponse à une demande spécifique. En pratique, le tribunal prend en compte le degré d'atteinte à la vie privée de l'individu soupçonné et de tiers au regard de l'intérêt de l'enquête.
Italie	90 jours	6 mois
Japon	60 jours	En cas de conservation des données sur la base de la coopération volontaire des FSI, la période de conservation peut dépasser 60 jours.
Lettonie	30 jours	Jusqu'à 90 jours
Liechtenstein	Aucune information n'a été fournie.	Aucune information n'a été fournie.
Lituanie	Aux termes de la Loi sur les communications électroniques, les fournisseurs de services sont tenus de conserver les données pendant 6 mois, avec possibilité de renouvellement pour une nouvelle période de 6 mois.	Aucune condition spécifique n'est requise pour étendre ou renouveler la période de conservation. Une demande de renouvellement suffit.
Luxembourg		
Malte	Conservation des données relatives à l'accès à l'internet et au courrier électronique pendant une période de six mois à partir de la date des communications. Conservation des données relatives au réseau de téléphonie fixe, au réseau de téléphonie mobile et au réseau internet pendant un an à partir de la date des communications.	

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période d'extension ou de renouvèlement de la conservation des données spécifiées
Maurice	Le temps jugé raisonnablement nécessaire pour enquêter sur une infraction ; en cas d'institution de poursuites, jusqu'à la conclusion de l'affaire ; ou encore la durée fixée par un juge dans une ordonnance.	Les conditions et la période d'extension ou de renouvellement sont régies par les dispositions de l'article 11(3) du CMCA.
Moldova	1 mois	Jusqu'à six mois
Monténégro	La législation ne prévoit pas de limite spécifique.	
Pays-Bas	90 jours	90 jours
Norvège	90 jours. Si les données sont conservées sur demande internationale, il n'est pas nécessaire de renouveler la période de conservation car celle-ci est généralement étendue par les autorités norvégiennes.	
Panama		
Pologne	Si les données sont conservées au titre d'une requête internationale, il n'est pas nécessaire de renouveler la période de conservation.	
Portugal	3 mois	Un an maximum
Roumanie	60 jours	30 jours
Serbie	Pas de législation sur la conservation des données.	
Slovaquie	90 jours	90 jours
Slovénie	Pas de législation sur la conservation des données.	
Espagne	90 jours	90 jours
Sri Lanka		
Suisse	90 jours	Les demandes de conservation des données peuvent être prolongées ou renouvelées à tout moment dans le délai exigé pour la soumission d'une demande formelle d'entraide judiciaire.
« L'ex-République yougoslave de Macédoine »		
Turquie	Bien que l'article 29/7 de la Convention de Budapest exige des Parties qu'elles conservent les données pendant au moins 60 jours, il n'existe pas de dispositions spécifiques sur les demandes de conservation et la	

Partie	Période de conservation des données suite à une demande étrangère	Conditions et période d'extension ou de renouvèlement de la conservation des données spécifiées
	durée de la période de conservation. Cependant, l'article 8/1-c de la Loi n° 6706, intitulé « Requête judiciaire étrangère », réglemente la conservation des preuves, y compris la conservation temporaire de données, pendant une période de 40 jours. Les données de trafic sont également conservées pendant une certaine période au titre de la Loi n° 5651. Aux termes de l'article 5/3 de la Loi n° 5651, les fournisseurs de services sont tenus de conserver les données de trafic de leurs services d'hébergement pendant au moins un an et deux ans maximum, conformément aux durées indiquées dans la réglementation ; ils doivent aussi assurer l'exactitude, l'intégrité et la confidentialité de ces données. En vertu de l'article 6/1-b de la Loi n° 5651, les fournisseurs d'accès sont tenus de conserver les données de trafic de leurs services pendant au moins six mois et deux ans maximum, conformément aux durées indiquées dans la réglementation ; ils doivent aussi assurer l'exactitude, l'intégrité et la confidentialité de ces données.	
Ukraine		
Royaume-Uni		
États-Unis d'Amérique	90 jours	90 jours

3.2 Aperçu général des suites données à la Recommandation

Le T-CY est conscient du fait que les différentes modalités d'application des mesures de conservation peuvent être source de confusion et de problèmes pour les États requérants. De plus, il est souvent difficile de traiter et de mener à bien une requête d'entraide judiciaire avant que s'achève la période de conservation des données, en particulier lorsque l'enquête continue à évoluer ou lorsque des raisons pratiques – délais de traduction, par exemple – entraînent des retards. Cette Recommandation a pour but de permettre aux États requérants de déterminer s'ils peuvent raisonnablement compter sur les données qu'ils cherchent à obtenir.

Les réponses des États à cette question se répartissent globalement en deux catégories selon qu'ils ont défini une période spécifique de conservation des données, ainsi que des conditions de renouvellement de cette période, ou qu'ils n'ont établi aucune limite de durée spécifique, souvent parce qu'ils ne disposent pas d'un texte de loi écrit régissant cette question[28].

La durée de la période de conservation des données varie en outre quelque peu parmi les États qui ont établi une limite à ce sujet. La majorité, cependant, ont opté pour une période plus longue :

- seuls quelques États prévoient une période de 60 jours ou moins (Japon, Lettonie, Roumanie) ;
- la plupart ont opté pour une période de 90 jours (Albanie, Bulgarie, Canada, Espagne, États-Unis, France, Hongrie, Italie, Pays-Bas, Portugal, Slovaquie) ou de 180 jours (Australie, Danemark, Lituanie, Malte).

Dans certains États, la durée de la période de conservation des données varie en fonction de la demande du procureur ou de l'État étranger concerné ou bien cette durée n'est pas spécifiquement limitée (Arménie, Autriche, Estonie, Maurice, Monténégro, Pologne, République tchèque, Serbie, Slovénie, Suisse) et, le cas échéant, les données peuvent donc être conservées indéfiniment.

Les fournisseurs de services internet peuvent décider de conserver les données pour une période plus longue que celle exigée par la législation pertinente.

La plupart des États autorisent le renouvellement de la période de conservation des données (parfois en exigeant une nouvelle requête formelle). Seuls la Bulgarie et le Japon déclarent qu'ils ne l'autorisent pas. Les États limitent parfois la durée totale de conservation des données, y compris en cas de renouvellement de la période initiale. Lorsqu'une telle limite existe, elle se situe presque toujours entre six mois et deux ans (Albanie, Australie, Canada, Espagne, États-Unis, France, Italie, Lituanie, Malte, Maurice, Pays-Bas, Portugal).

3.3 Conclusion

Des périodes plus longues visent à assurer la conservation des données pendant que les Parties préparent leurs requêtes d'entraide judiciaire. Pour ce faire, une période initiale assez longue, associée à la possibilité de renouveler facilement cette période ou de conserver indéfiniment les données, est nécessaire. Pour éviter les erreurs à ce sujet, les Parties devraient vérifier au préalable auprès de leurs partenaires étrangers les conditions exactes de conservation des données. Il serait également utile que les Parties facilitent l'accès à toutes les informations relatives à la conservation des données.

[28] L'Allemagne, l'Azerbaïdjan, la Belgique, Chypre, la Croatie, la Finlande, la Géorgie, l'Islande, le Luxembourg, Moldova, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et Ukraine n'ont pas répondu à cette question.

4 Recommandations 17 et 18

4.1 Rec 17 – Formulaires plurilingues

> Rec 17 – Le Conseil de l'Europe devrait – de par ses projets de renforcement des capacités – élaborer ou créer des liens vers des formulaires modèles standardisés, plurilingues pour les demandes au titre de l'article 31.

4.1.1 Suites données à la Recommandation

Dans le cadre du projet Cybercriminality@EAP II, le Conseil de l'Europe a mis au point en 2016 des projets de formulaires types de demande de conservation des données à utiliser dans les requêtes au titre des articles 29 et 30 de la Convention de Budapest et dans les demandes de données informatiques (informations sur les abonnés, données de trafic, données sur le contenu) adressées au titre de l'article 31 de la Convention de Budapest.

Ces formulaires types ont été développés lors d'activités menées avec les États du Partenariat oriental (Arménie, Azerbaïdjan, Belarus, Géorgie, Moldova and Ukraine), avec le soutien d'experts de France, d'Allemagne, du Portugal, de « l'ex-République yougoslave de Macédoine » et du Royaume-Uni.

Le formulaire type de demande de préservation de données aurait été testé en pratique par la Géorgie et Moldova. La France a adapté et modifié le formulaire type en vue de son utilisation concrète.

Dans ces formulaires types, la part du texte est limitée ; ils contiennent principalement des cases à cocher. Cela facilitera leur conversion en formulaire plurilingue.

4.1.2 Conclusion

Des progrès positifs ont été réalisés dans la mise au point des modèles de formulaires.

Il est recommandé que des experts du T-CY examinent ces modèles de formulaires et les communiquent ensuite au T-CY et aux points de contact 24/7 pour commentaires.

4.2 Rec 18 – Ressources en ligne

> 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.

4.2.1 Suites données à la Recommandation

La Division de cybercriminalité du Secrétariat (Secrétariat du T-CY et Bureau du Programme du Conseil de l'Europe sur la cybercriminalité, C-PROC) a commencé à mettre sur pied la Communauté Octopus en 2014, y compris un outil consacré à la coopération internationale.

Les progrès accomplis en ce domaine ont été présentés au T-CY 14 les 1-2 décembre 2015 et le T-CY a salué « la création de la Communauté Octopus sur la cybercriminalité, en appelant les

membres et les observateurs du T-CY à contribuer à l'élaboration des outils mis à disposition sur cette plateforme ».

En 2016, le Secrétariat a sollicité les données nécessaires des Parties à la Convention. Les données reçues ont été téléchargées. En avril 2017, sur 54 Parties, 16 avaient fourni des informations complètes, 21 avaient fourni des informations partielles ou incomplètes et 17 n'avaient pas encore contribué à la Communauté Octopus.

Certains facteurs techniques empêchent encore de faire de cet outil une application facile à utiliser, notamment des capacités insuffisantes en termes de contenus, le manque de flexibilité du système de gestion des contenus qui nuit à l'expérience des usagers, ainsi que les questions d'accessibilité et de sécurité de la plateforme. Le Secrétariat du T-CY examine actuellement des propositions de sous-traitance de la Communauté Octopus afin de surmonter les problèmes techniques et de permettre à la Communauté de continuer à évoluer.

4.2.2 Conclusion

Des progrès importants ont été réalisés dans la mise en place d'un outil qui, une fois pleinement opérationnel, apportera beaucoup à la coopération internationale en matière de cybercriminalité et de preuves électroniques.

Les Parties sont invitées à fournir au Secrétariat du T-CY les données nécessaires pour compléter l'information concernant leurs autorités et procédures respectives. Des efforts supplémentaires devraient être engagés pour assurer la mise à disposition d'informations complètes sur toutes les Parties.

Compte tenu des capacités internes limitées pour résoudre les problèmes techniques et soutenir la poursuite du développement de la Communauté Octopus, l'option de sous-traitance devrait être poursuivie. Les Parties et les donneurs devraient envisager le versement de contributions volontaires pour soutenir l'évolution continue de la Communauté Octopus.

5 Conclusions, recommandations et suivi

5.1 Conclusions

- L'entraide judiciaire est et restera l'un des principaux moyens de recueillir des preuves électroniques dans les procédures pénales. Tout en recherchant de nouvelles solutions pour les cas où l'entraide judiciaire n'est pas une option, les États doivent prendre les mesures nécessaires pour améliorer l'efficience de l'entraide judiciaire lorsqu'elle peut être obtenue. Les suites données aux Recommandations adoptées par le T-CY en décembre 2014 contribueront à la réalisation de cet objectif.

- Le T-CY se réjouit du fait que 40 Parties et Observateurs ont communiqué de nombreuses informations sur les suites données à ces Recommandations. Le Comité note cependant que, dans certains cas, des compléments d'information seraient utiles pour comprendre pleinement la situation factuelle et juridique dans un pays. Le T-CY regrette que certaines Parties n'aient pas répondu au questionnaire.

- Les informations reçues montrent que de nombreux États ont donné suite à un grand nombre des Recommandations. Les bonnes pratiques décrites au regard des différentes Recommandations pourront servir d'inspiration aux autres États.

- Les informations reçues donnent parfois une image assez optimiste du fonctionnement de l'entraide judiciaire. Les États déclarent qu'ils s'efforcent d'assurer que leurs requêtes d'entraide judiciaire sont exactes et complètes mais s'inquiètent du fait qu'il n'en va pas de même pour les requêtes qu'ils reçoivent. Cela laisse à penser qu'il serait nécessaire que le T-CY engage des efforts supplémentaires pour suivre le fonctionnement de l'entraide judiciaire dans la pratique.

- De nombreux États déclarent tenir des statistiques sur la cybercriminalité et les preuves électroniques aux fins de l'entraide judiciaire. Il serait utile que les États partagent ces données avec le T-CY.

5.2 Recommandations

Les suites supplémentaires à donner aux Recommandations adoptées par le T-CY sont décrites ci-dessous :

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 des données (suite au rapport d'évaluation de 2012 du T-CY).

Autres suites à donner à la Recommandation :

- ► Les Parties devraient supprimer les obstacles à l'exécution des demandes internationales de conservation des données, en particulier eu égard aux requêtes d'entraide judiciaire (Hongrie, Maurice, République tchèque, Serbie, Turquie) ou afin de renforcer la conformité (Bosnie et Herzégovine, Liechtenstein)[29].
- ► Les Parties devraient engager les réformes nécessaires pour introduire dans leur législation nationale des dispositions spécifiques sur la conservation des données, comme recommandé par le T-CY dans les rapports d'évaluation sur la mise en

[29] Chypre, la Géorgie, l'Islande, le Luxembourg, le Panama, « l'ex-République yougoslave de Macédoine », le Royaume-Uni, le Sri Lanka et l'Ukraine n'ont pas répondu à cette question.

œuvre rapide des dispositions de la Convention en matière de conservation des données[30].

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.

Autres suites à donner à la Recommandation :

- Les Parties devraient communiquer des statistiques et des études de cas au Secrétariat du T-CY pour permettre l'évaluation continue par le T-CY du fonctionnement de l'entraide judiciaire en ce qui concerne la cybercriminalité et les preuves électroniques. Le T-CY devrait faciliter l'échange de bonnes pratiques pour encourager les Parties à tenir des statistiques.

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 (comme les Bureaux locaux des procureurs).

Autres suites à donner à la Recommandation :

- Les États devraient poursuivre et envisager d'intensifier leurs efforts en vue d'affecter du personnel formé aux technologies aux fins de l'entraide judiciaire, pour assurer l'efficience des procédures au niveau du centre et des régions.

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.

Autres suites à donner à la Recommandation :

- Les États devraient examiner la possibilité d'adopter une approche systématique de la formation à l'entraide judiciaire et à d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques.
- Le Conseil de l'Europe (Secrétariat du T-CY ou C-PROC) devrait établir une liste des formateurs et des institutions capables de fournir une formation standardisée et reproductible à la coopération internationale en matière de cybercriminalité et de preuves électroniques.

Rec 5 Les Parties et le Conseil de l'Europe devraient travailler à renforcer le rôle des points de contact 24/7 conformément à l'article 35 de la Convention de Budapest, notamment :

g. veiller, conformément à l'article 35.3 de la 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 ;
h. veiller à ce que les points de contact promeuvent activement leur rôle parmi les autorités nationales et leurs homologues étrangères ;

[30] Rapport d'évaluation sur la mise en œuvre des dispositions de la Convention de Budapest en matière de conservation des données :
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e
Rapport d'évaluation supplémentaire sur la mise en œuvre des dispositions de la Convention de Budapest en matière de conservation des données :
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

i. assurer entre les Parties des réunions régulières et la formation du réseau 24/7 ;
j. 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'État requérant ;
k. 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 ;
l. les points de contact 24/7 devraient jouer un rôle de soutien pour les demandes « article 31 ».

Suites à donner à la Recommandation :

- Les États devraient prendre de nouvelles mesures pour améliorer la coopération entre les points de contact 24/7 et les autorités chargées de l'entraide judiciaire.
- Le T-CY devrait discuter de cas concrets impliquant des points de contact 24/7 afin de résoudre les problèmes existants.
- Le Conseil de l'Europe devrait organiser des ateliers ou des sessions de formation pour les points de contact 24/7 créés conformément à l'article 35 pour faciliter le fonctionnement du réseau.

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. À cet égard, les Parties doivent partager les bonnes pratiques avec le T-CY.

Suites à donner à la Recommandation :

- Les États devraient examiner la possibilité d'adopter – en s'appuyant sur l'expérience d'autres États – de nouvelles mesures pour réduire le nombre d'étapes requises pour l'entraide judiciaire.

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.

Suites à donner à la Recommandation :

- Les États devraient envisager de développer de nouveaux canaux de coopération informels dans les limites autorisées par la législation pertinente.

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 services.

Suites à donner à la Recommandation :

- Les États devraient sensibiliser les décideurs à l'augmentation du nombre de situations dans lesquelles une procédure d'urgence est requise pour permettre la divulgation rapide de preuves électroniques. Les projets de renforcement des capacités du Conseil de l'Europe devraient faciliter la sensibilisation des décideurs à ce sujet.
- Les États devraient améliorer et formaliser les procédures d'urgence concernant la divulgation de preuves électroniques. Pour ce faire, les décideurs devront également être sensibilisés à cette nécessité.
- L'introduction de dispositions relatives aux procédures d'urgence – via l'entraide judiciaire et la coopération directe avec les fournisseurs de données – devrait en outre être envisagée dans l'élaboration du Protocole à la Convention de Budapest.

Rec 9 Les Parties devraient accuser réception des demandes systématiquement et notifier, sur demande, les actions prises.

Suites à donner à la Recommandation :

- ► Les points de réception des requêtes d'entraide judiciaire devraient systématiquement en accuser réception et indiquer la personne à contacter pour le suivi.

Rec 10 Les Parties devraient envisager l'ouverture d'une enquête nationale sur demande étrangère ou information spontanée pour faciliter le partage d'information ou accélérer l'entraide judiciaire.

Suites à donner à la Recommandation :

- ► Les États devraient fournir des informations supplémentaires sur la mise en œuvre de cette Recommandation, y compris l'utilisation de l'information spontanée.

Rec 11 Les Parties devraient utiliser la transmission électronique des demandes conformément à l'article 25.3 de la Convention de Budapest relatif aux moyens rapides de communication.

Suites à donner à la Recommandation :

- ► Les États devraient supprimer les obstacles à la transmission électronique des demandes.

Rec 12 Les Parties veillent à ce que les demandes soient spécifiques et contiennent toutes les informations nécessaires.

Suites à donner à la Recommandation :

- ► Les États devraient communiquer au T-CY des exemples de difficultés causées par des requêtes d'entraide judiciaire inadéquates. Cela permettrait de mettre en regard le point de vue des États au sujet des demandes reçues et envoyées.

Rec 13 Conformément à l'article 25.5 de la 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 pour faciliter l'octroi de l'aide.

Suites à donner à la Recommandation :

- ► Les États devraient continuer à faire preuve de flexibilité dans l'application des normes de double incrimination.

Rec 14 Les Parties sont encouragées à consulter les autorités de la Partie requise avant d'envoyer les demandes, quand cela est nécessaire.

Suites à donner à la Recommandation :

- ► Les États devraient recourir plus fréquemment à l'option consistant à consulter au préalable les autorités de la Partie requise, afin de réduire au minimum les erreurs, les retards et les coûts.

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.

Suites à donner à la Recommandation :

- ► Les États devraient engager des efforts supplémentaires pour mettre en œuvre cette Recommandation. Ils devraient aussi s'appuyer sur la Communauté Octopus à cet égard.

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 préservation étrangère conformément à l'article 29 Convention de Budapest. Le T-CY devrait documenter les périodes de conservation.

Suites à donner à la Recommandation :

- ► Les Parties devraient assurer l'accès facile aux renseignements relatifs à la période de conservation des données et à d'autres conditions sur leurs sites web concernant l'entraide judiciaire, ainsi que via la Communauté Octopus.
- ► Le T-CY considère qu'une période de conservation des données de moins de 90 jours, avec possibilité de renouvellement d'au moins une fois, n'est pas suffisante.

Rec 17 Le Conseil de l'Europe devrait – de par ses projets de renforcement des capacités – élaborer ou créer des liens vers des formulaires modèles standardisés, plurilingues pour les demandes au titre de l'article 31.

Suites à donner à la Recommandation :

- ► Des experts sélectionnés parmi les membres du T-CY devraient passer en revue les modèles préparés dans le cadre des projets de renforcement des capacités, puis les communiquer au T-CY et aux points de contact 24/7 pour commentaires et adoption.
- ► Les modèles devraient ensuite être finalisés et mis à la disposition des Parties via la Communauté Octopus.

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.

Suites à donner à la Recommandation :

- ► Les Parties devraient fournir les informations requises via l'outil en ligne sur la coopération internationale de la Communauté Octopus.
- ► Le Conseil de l'Europe devrait envisager de sous-traiter la Communauté Octopus pour résoudre certains problèmes techniques et favoriser la poursuite de l'évolution de ses outils. Les Parties et les donneurs devraient réfléchir à la possibilité de verser des contributions volontaires à cette fin.

5.3 Suivi

Le partage d'affaires, d'expériences et d'observations concernant l'entraide judiciaire et d'autres formes de coopération internationale devrait devenir un élément régulier des sessions plénières du T-CY.

Les Parties et les Observateurs sont invités à notifier le T-CY des suites données aux Recommandations au cours des sessions plénières.