



Strasbourg, le 18 février 2009
[PC-OC Docs/(2009)05f Synthese. Rép.]

PC-OC (2009) 05

COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS
(CDPC)

Comité d'experts
sur le fonctionnement des conventions européennes
sur la coopération dans le domaine pénal
(PC-OC)

**Synthèse des réponses au questionnaire sur
l'entraide judiciaire dans les affaires liées à l'informatique**

Informations générales :

Le Comité de la Convention Cybercriminalité (T-CY) a évoqué, à sa deuxième réunion tenue à Strasbourg les 13 et 14 juin 2007, les difficultés actuelles relatives à l'entraide judiciaire en vertu de la Convention sur la cybercriminalité. Il est convenu que les Etats parties devaient coopérer dans les délais impartis pour que la lutte contre la cybercriminalité soit efficace. Il a entre autres souligné que la Convention était applicable aux délits commis dans un but terroriste et qu'à cet égard la courte période de conservation des données entraînait des problèmes d'ordre pratique importants pour les autorités compétentes.

Le T-CY a noté que les délinquants avaient recours à toutes les possibilités offertes par le cyberspace, ce qui rend la mission des services répressifs plus difficile étant donné que les affaires de cybercriminalité impliquent souvent plus de deux Etats. Il a été souligné qu'au cours des enquêtes sur les délits commis par le biais de l'Internet, les méthodes classiques d'entraide judiciaire, et en particulier ses limites de temps, ne pouvaient pas toujours répondre aux objectifs de la Convention. Dans le contexte des crimes informatiques, les données informatiques censées servir d'éléments de preuve, peuvent être détruites/perdus instantanément, et dans ces conditions la période de 90 jours paraît inappropriée.

Le T-CY ayant demandé des conseils de bonnes pratiques en matière d'entraide judiciaire dans les affaires liées à l'informatique (notamment les affaires urgentes), le CDPC a chargé le PC-OC de fournir les conseils pratiques demandés et d'examiner les points relatifs aux questions opérationnelles comme l'article 32 b de la Convention, qui énonce la disposition suivante :

« Une Partie peut, sans l'autorisation d'une autre Partie [...] accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. »

Le PC-OC a adopté un questionnaire sur la question et il l'a envoyé à tous les Etats membres et observateurs du Conseil de l'Europe.

Vingt et un Etats membres, plus le Canada et le Japon, ont répondu au questionnaire. Ces réponses sont données dans le document PC-OC (2008) 08 Rev disponible sur le site web du PC-OC (www.coe.int/tcj).

Les pages qui suivent donnent un récapitulatif de ces réponses. L'Annexe donne un tableau des signatures et ratifications de la Convention sur la cybercriminalité.

Question 1 :

Veillez présenter les méthodes, les moyens et les outils utilisés par les autorités compétentes de votre pays pour fournir une assistance judiciaire aux autorités d'autres États dans les affaires urgentes (voies de communication, traduction, etc.). Veillez donner des exemples de bonnes pratiques ou des indications qui visent à renforcer l'efficacité de cette entraide judiciaire dans les affaires urgentes, notamment dans les affaires liées à l'informatique (cybercriminalité).

Les États ayant répondu au questionnaire n'ont pas tous fourni des informations précises sur les moyens de communication qui peuvent être utilisés pour demander l'entraide judiciaire dans les affaires liées à l'informatique. Un certain nombre d'entre eux ont explicitement déclaré que les autorités compétentes de l'État requérant pouvaient transmettre leurs demandes d'entraide judiciaire directement à leurs homologues de l'État requis. Cette possibilité est envisagée dans la législation nationale de certains États (par exemple la Bulgarie et la République tchèque). Quatre États¹ ont noté que les contacts directs entre autorités compétentes sont possibles, à condition que les coordonnées des autorités compétentes requises soient disponibles et qu'il existe un traité approprié (comme notamment la Convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne ou le Deuxième protocole additionnel à la Convention européenne relative à l'entraide judiciaire en matière pénale) et la réciprocité. Au Luxembourg, bien que la demande directe d'entraide judiciaire adressée aux autorités juridiques ne soit pas prévue dans la législation nationale, elle n'en est pas moins admise en pratique, notamment en cas d'urgence.

Dans certains États membres, les demandes doivent être adressées à une autorité centrale². La Bosnie-Herzégovine a déclaré qu'elle soumet ses demandes d'entraide judiciaire par la voie diplomatique. Le Japon utilise la voie diplomatique lorsqu'il est le pays requérant, sauf lorsqu'il existe un traité bilatéral d'entraide judiciaire.

La majorité des États ayant répondu³ ont déclaré que, dans les affaires urgentes, leurs autorités compétentes utilisent essentiellement les réseaux de communication de la police et des instances juridiques (INTERPOL, Europol, Eurojust, le Réseau judiciaire européen, ou le PC-OC). Six États membres⁴ évoquent le Réseau 24/7 constitué au titre de l'article 35 de la Convention sur la cybercriminalité et la Lettonie et la Slovaquie mentionnent le Réseau I-24/7 d'INTERPOL. Le Japon dit utiliser le réseau 24/7 de points de contacts établis dans le cadre du plan d'action du G8 pour la lutte contre la criminalité liée à la haute technologie.

Pour ce qui est des moyens de communication, tous les États membres qui ont fourni des détails sur cet aspect de la coopération, ainsi que le Canada et le Japon, ont déclaré que les moyens de communication modernes qui laissent des traces écrites, comme les fax et les courriers électroniques, sont acceptables, au moins dans les affaires urgentes.

La majorité des États ayant répondu n'ont pas donné d'informations sur leurs prescriptions en matière de langue. Certains États⁵ demandent des traductions dans leur(s) langue(s) officielle(s) ou en anglais. Bien que la législation suédoise dise que les demandes d'assistance juridique et les documents les accompagnant soient traduites en suédois, danois ou norvégien, les autorités compétentes peuvent accorder des dérogations à cette prescription. Le Japon a répondu que, bien qu'il requière que la demande soit accompagnée d'une traduction en japonais, il accepte les demandes en anglais en cas d'urgence.

¹ Pologne, Slovaquie, Slovénie, Suède

² Bosnie-Herzégovine, Malte (Bureau du procureur général), Turquie (Ministère de la justice, Direction générale du droit international et des relations extérieures), Ukraine (Ministère de la justice pour les demandes adressées aux tribunaux, au Bureau du procureur général pour les demandes aux instances d'instruction).

³ Arménie, Finlande, Grèce, Hongrie, Lettonie, Lituanie, Malte, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Turquie, Ukraine.

⁴ Arménie, Finlande, Hongrie, Lettonie, Lituanie, Roumanie.

⁵ Bulgarie (en une des langues officielles du Conseil de l'Europe), Finlande (les demandes en d'autres langues sont acceptables mais peuvent être cause de retards) Luxembourg et Suisse.

L'Allemagne et la Lituanie sont d'avis qu'une traduction dans une langue acceptable et largement reconnue de l'État requis, même si elle n'est pas obligatoire, accélère le traitement de la demande. La Pologne déclare qu'en pratique, les demandes urgentes sont transmises entre les autorités compétentes avec leur traduction.

Pour ce qui est des exemples de bonne pratique et des lignes directrices concernant les affaires urgentes liées à l'informatique, la plupart des États ayant répondu n'ont pas fait de commentaires précis. L'Arménie et la Slovénie ont déclaré qu'elles n'ont aucune expérience en matière de coopération dans les affaires urgentes liées à l'informatique, qu'elles soient fondées sur la Convention sur la cybercriminalité ou d'autres traités.

La Bosnie-Herzégovine mentionne le procès de deux personnes ayant commis des fraudes sur l'Internet ainsi que la vérification des adresses IP à la suite d'informations reçues du bureau INTERPOL de Wiesbaden.

La Lettonie pense que l'utilisation du système de communications I-24/7 d'INTERPOL est la solution optimale et mentionne deux cas de coopération couronnée de succès sur la base de demandes qu'elle a faites par l'intermédiaire du bureau américain d'INTERPOL. La Slovaquie déclare aussi que le réseau I-24/7 d'INTERPOL et le système slovaque de juges et de procureurs de garde constituent un cadre efficace de traitement des affaires urgentes.

La Lituanie souligne que l'on obtient les meilleurs résultats lorsque les agents responsables ont l'occasion de discuter du plan et du processus d'exécution ainsi que des questions pratiques et juridiques liées à une demande directement lors de réunions de coordination.

La Pologne souligne qu'elle encourage ses autorités judiciaires à transmettre directement les demandes d'entraide judiciaire à leurs homologues, chaque fois que cela est possible.

Dans sa réponse très complète au questionnaire, la Roumanie mentionne un certain nombre de cas pratiques qui illustrent certains problèmes. Elle parle notamment d'une affaire concernant des délits multiples touchant 12 pays sur trois continents au cours de laquelle sont apparues des différences manifestes dans la célérité et l'attention dont ses demandes d'entraide ont été traitées par les différents pays. Elle déclare qu'au niveau des procès, la majorité des demandes porte sur la délivrance d'assignations ou de documents, suivie par les demandes d'audition de témoins. Une des difficultés qu'elle a rencontrées tient au fait que, lorsque des moyens de communication rapides sont utilisés dans les affaires urgentes, de nombreux pays refusent de traiter les demandes tant qu'ils n'ont pas reçu de copies certifiées. La Roumanie suggère certaines lignes directrices possibles :

- possibilité de demandes directes entre les autorités compétentes et possibilité d'utiliser des moyens de communication modernes ;
- importance des réseaux pour encourager les contacts humains indispensables dans les affaires urgentes, et nécessité d'avoir facilement accès aux coordonnées ;
- possibilité de créer un réseau mondial de soutien des victimes (permettant la représentation des victimes d'un autre État, et d'éviter ainsi les retards liés à la remise des documents ;
- nécessité pour les États où résident les victimes de traiter tous les cas de cybercriminalité avec célérité, quels qu'en soient les dommages.

Le Canada, comme la Roumanie, souligne l'importance d'une autorité centrale bien définie, facilement joignable et disponible en permanence. Il pense que, dans la mesure du possible, les États devraient avoir recours à des magistrats de liaison détachés à l'extérieur, capables d'offrir des conseils dès le début des affaires. Il attire aussi l'attention sur la nécessité de présenter des demandes complètes et précises contenant toutes les informations requises, dont les raisons de l'urgence et les priorités, ainsi que les noms des personnes, comme les agents de police, déjà contactées pour l'affaire. À ce propos, le Canada souligne la valeur d'une coopération informelle entre les autorités de police.

Question 2 :

Si votre Etat est partie à la Convention sur la cybercriminalité, veuillez indiquer comment l'article 32 b de cette Convention est appliqué ou est censé être appliqué dans la pratique dans le cadre de votre juridiction ? Comment les autorités compétentes de votre pays interprètent-elles les dispositions de l'article mentionné dans la législation et/ou dans la pratique ?

Tous les États ayant répondu (à l'exception de la Turquie) sont signataires de la Convention sur la cybercriminalité et 11 d'entre eux⁶ l'ont déjà ratifiée. Il semble, de l'expérience de ces pays, que les dispositions de la Convention sur la cybercriminalité, et plus précisément celles du chapitre III sur la coopération internationale, n'ont jamais été utilisées comme fondement légal exclusif pour la transmission d'une demande d'assistance juridique dans les affaires liées à l'informatique. La Roumanie pense que cela peut être dû aux dispositions de la Convention elle-même et notamment à celles du paragraphe 4 de l'article 25 qui dit que « l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables ». Les principaux traités les plus souvent cités dans ce contexte sont la Convention européenne d'entraide judiciaire en matière pénale, et, pour ce qui est des membres de l'Union européenne, la Convention relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, suivis par les traités bilatéraux et la Convention des Nations unies contre la criminalité transnationale organisée.

Aucun des États ayant répondu ne fait état d'une expérience concrète de l'application de l'article 32 b de la Convention et aucun ne ressent la nécessité de modifier sa législation à la lumière de cet article. L'Arménie ne voit pas la nécessité de mettre immédiatement cet article en œuvre, préférant se concentrer sur « les opportunités des points de contact 24/7 ». Si la Grèce a préparé un projet de loi relative à la ratification et à la mise en œuvre de la Convention, son texte ne traite pas de cet article.

La Bulgarie et la Slovénie soulignent que la Convention est directement applicable dans leur système interne et que l'article 32 b sera interprété et appliqué à la lumière du rapport explicatif et dans l'esprit de la Convention, ainsi que du « droit national et international sur la protection des données ».

Seuls cinq États⁷ ont fait des commentaires sur le contenu et l'interprétation de l'article 32 b, et leurs point de vue sont très divergents.

Pour l'Allemagne, la Finlande et la Lettonie, les dispositions de cet article prévoient l'accès transfrontière sans l'autorisation du pays où les données informatiques sont stockées, mais leur interprétation diffère ensuite sur ce qui est permis.

L'Allemagne, bien qu'elle ne soit pas partie à la Convention, interprète cette disposition comme autorisant les autorités du pays A à accéder à des données non accessibles au public stockées dans un pays B sans adresser une demande d'entraide judiciaire si la personne du pays B qui est légalement autorisée à transmettre ces données aux autorités nationales a donné son consentement légal et volontaire à cet accès. Cet « acte souverain » est compatible avec la procédure pénale allemande et n'est pas considéré comme une exception à l'entraide judiciaire formelle.

La Lettonie considère que le propriétaire ou l'opérateur d'un système informatisé peut fournir des données informatisées stockées directement aux autorités compétentes d'un autre État s'il a reçu une autorisation écrite de l'utilisateur ou de l'abonné à cet effet.

La Finlande interprète cette clause de manière plus restrictive. À son avis, l'article 32 b autorise « à accéder, par exemple, le courrier électronique de la personne concernée si elle en a donné la permission légale », sans la participation, l'assistance ou le rôle actif de l'autre Partie. Cependant, la Finlande considère que cela ne s'applique pas quand les informations proviennent d'un fournisseur de services (comme Google) : dans ces cas, il faut utiliser les modalités ordinaires de l'entraide judiciaire.

⁶ Arménie, Bosnie-Herzégovine, Bulgarie, Finlande, Hongrie, Lettonie, Lituanie, Roumanie, Slovaquie, Slovénie, Ukraine.

⁷ Allemagne, Finlande, Lettonie, Slovaquie, Ukraine.

La Slovaquie et l'Ukraine, en revanche, ont des interprétations plus restrictives de cette disposition (La Slovaquie la considère comme l'une des plus progressives et des plus difficiles de la Convention).

Pour la Slovaquie, l'autorisation d'une autorité juridique compétente de la Partie où sont stockées les données informatiques (qu'elle considère comme l'État quasi-requis) est nécessaire dans tous les cas.

L'Ukraine pense que la mise en œuvre de l'article 32 b n'est possible que si les données concernées sont transmises par les autorités du pays où elles sont stockées. Elle est d'avis que l'accès transfrontière de ces données sans la connaissance ou le consentement de leur propriétaire constituerait une violation du droit du pays concerné.

Annexe

Convention sur la cybercriminalité (STE no. : 185)
Etat des signatures et ratifications
(Situation au 23/2/2009)

Etats membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	23/11/2001	20/6/2002	1/7/2004				X			
Allemagne	23/11/2001									
Andorre										
Arménie	23/11/2001	12/10/2006	1/2/2007				X			
Autriche	23/11/2001									
Azerbaïdjan	30/6/2008				X	X	X	X		
Belgique	23/11/2001									
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006				X			
Bulgarie	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Chypre	23/11/2001	19/1/2005	1/5/2005							
Croatie	23/11/2001	17/10/2002	1/7/2004				X			
Danemark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Espagne	23/11/2001 r									
Estonie	23/11/2001	12/5/2003	1/7/2004				X			
Finlande	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Géorgie	1/4/2008									
Grèce	23/11/2001									
Hongrie	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Irlande	28/2/2002									
Islande	30/11/2001	29/1/2007	1/5/2007		X		X			
Italie	23/11/2001	5/6/2008	1/10/2008				X			
Lettonie	5/5/2004	14/2/2007	1/6/2007		X		X			
l'ex-République yougoslave de Macédoine	23/11/2001	15/9/2004	1/1/2005				X			
Liechtenstein	17/11/2008									
Lituanie	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malte	17/1/2002									
Moldova	23/11/2001									
Monaco										
Monténégro	7/4/2005			55						
Norvège	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Pays-Bas	23/11/2001	16/11/2006	1/3/2007				X	X		
Pologne	23/11/2001									
Portugal	23/11/2001									
République tchèque	9/2/2005									
Roumanie	23/11/2001	12/5/2004	1/9/2004				X			
Royaume-Uni	23/11/2001									
Russie										
Saint-Marin										
Serbie	7/4/2005			55						
Slovaquie	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovénie	24/7/2002	8/9/2004	1/1/2005				X			

Suède	23/11/2001									
Suisse	23/11/2001									
Turquie										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			

Etats non membres du Conseil de l'Europe

Etats	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Afrique du Sud	23/11/2001									
Canada	23/11/2001									
Costa Rica										
Etats-Unis	23/11/2001	29/9/2006	1/1/2007		X	X	X			
Japon	23/11/2001									
Mexique										
Philippines										
République dominicaine										

Nombre total de signatures non suivies de ratifications :	23
Nombre total de ratifications/adhésions :	23