COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

**www.coe.int/cybercrime**

Strasbourg, le 25 mai 2021

T-CY (2021)12

## Comité de la Convention sur la cybercriminalité (T-CY)

**Préparation d'un 2e Protocole additionnel à la Convention de Budapest sur la cybercriminalité**

# Résumé des commentaires sur les avis des Comités du Conseil de l'Europe et les soumissions d'autres parties prenantes sur le projet de 2e Protocole additionnel à la Convention sur la cybercriminalité (mai 2021)

**Note préparé par le Secrétariat**

# Contenu



## Contact


M. Alexander Seger
Secrétaire du Comité de la Convention sur la Cybercriminalité (T-CY)
Direction générale Droits de l'Homme et État de droit
Conseil de l'Europe, Strasbourg, France
Courriel : alexander.seger@coe.int

# 1 Introduction

Le 12 avril 2021, la plénière de rédaction du protocole du Comité de la Convention sur la cybercriminalité (T-CY) a décidé de publier un dispositif complet et un Rapport explicatif préliminaire du projet de 2e protocole additionnel à la Convention de Budapest sur la cybercriminalité pour mener des consultations avec les comités pertinents du Conseil de l'Europe ainsi qu'avec les parties prenantes de la société civile, du secteur privé et des experts en protection des données.

La réunion en ligne, qui s'est tenue le 6 mai 2021, a mis un point final à la sixième série de consultations des parties prenantes sur ce protocole depuis juillet 2018. En ce qui concerne cette dernière série de consultation, des rapports écrits ont été communiqués par : Access Now, ADC, Canada Privacy Commission, CCBE, CENTR, CS Coalition, EuroISPA, EDPB, FRA, ICANN, Kaspersky, MARQUES, et New Zealand Privacy Commissioner.

En outre, des avis écrits ont été transmis par le Comité européen pour les problèmes criminels (CDPC) du Conseil de l'Europe et le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD).

Le présent résumé a pour objet de fournir des commentaires informels sur certaines des questions soulevées par les parties prenantes[1]. Compte tenu du grand nombre de points évoqués dans les soumissions et lors de la réunion du 6 mai, il ne sera pas possible ici de fournir des réponses détaillées à chacun d'entre eux.

# 2 Commentaire général sur les soumissions reçues

- Les contributions reçues au cours des cinq précédentes séries de consultations depuis 2018 ont contribué à façonner le Protocole au fur et à mesure de son évolution. En conséquence, certains outils n'ont pas été inclus dans le Protocole et le système de garanties a été renforcé. Le Protocole contient désormais un article détaillé sur la protection des données à caractère personnel.

- Des experts des Parties à la Convention sur la cybercriminalité de toutes les régions du monde ont participé aux négociations. Un grand nombre de réunions ont été tenues pour élaborer ce Protocole, dont la plupart étaient consacrées aux conditions et garanties applicables. On note que plus de soixante réunions en ligne ont eu lieu depuis le début de la pandémie de covid-19. Les délégations participant à ces réunions comprenaient des experts en protection des données.

- Le Protocole a pour objet de fournir des outils permettant d'enquêter sur les infractions et d'obtenir justice pour les victimes. Étant donné la prévalence de la cybercriminalité dans le monde d'aujourd'hui et le nombre relativement faible de sanctions pénales prononcées contre des cybercriminels, il est important de montrer aux victimes d'actes criminels en ligne que la justice tient de plus en plus compte de leurs attentes.

[1] Note : Ces commentaires informels concernent les contributions des intervenants mais ne reflètent pas nécessairement les avis des rédacteurs du Protocole, lesquels sont exposés dans le Rapport explicatif du Protocole.

- Le Protocole est un traité de justice pénale qui s'applique à des enquêtes ou procédures pénales spécifiques liées à la cybercriminalité et au recueil de preuves sous forme électronique (voir l'article 2 – Champ d'application). Il ne s'agit pas d'un instrument utilisé à des fins de sécurité nationale, ni d'un instrument de surveillance de masse ou de collecte massive de données en masse, ni encore d'un traité visant à établir ou harmoniser des régimes complets de protection des données.

- Il s'agit d'un protocole additionnel (et non d'un protocole d'amendement) et un État ne peut devenir Partie que s'il a adhéré à la Convention et souscrit à ses normes, y compris ses conditions et garanties (article 15), en premier lieu.

- Ni la Convention de Budapest ni le Protocole ne contiennent de dispositions exigeant une conservation indifférenciée des données par les fournisseurs pendant une période définie. En revanche, la Convention comprend des mesures qui s'appliquent à la conservation de données nécessaires dans le contexte d'une enquête ou d'une procédure pénale spécifique.

- Les outils du Protocole ne seront pas appliqués de manière isolée par les Parties mais devront être mis en œuvre et intégrés dans le cadre juridique interne d'une Partie. Les systèmes de justice pénale des Parties prévoient des conditions, des garanties et des mécanismes de supervision.

- La Convention de Budapest est un traité qui compte actuellement 66 Parties (dont 21 qui ne sont pas des États membres du Conseil de l'Europe et 40 qui ne sont pas membres de l'Union européenne). Le Protocole doit s'appliquer à tous ces pays ainsi qu'à ceux qui souhaitent devenir Parties. Les dispositions doivent être claires, suffisamment spécifiques et détaillées, tout en laissant une marge de manœuvre suffisante pour permettre une adaptation aux différents systèmes juridiques et à l'évolution de la technologie, des modèles économiques et de l'interprétation par les tribunaux.

- Bien que les Parties à la Convention aient créé un mécanisme qui permet de procéder, par l'intermédiaire du T-CY, à des évaluations de la mise en œuvre de la Convention, ces évaluations deviendront, au titre du présent Protocole, une exigence du traité en vertu de l'article 23.

# 3 Avis des comités du Conseil de l'Europe

## 3.1 Comité européen pour les problèmes criminels (CDPC),

### 3.1.1 Résumé des points soulevés par le CDPC

À la demande du Secrétariat du T-CY, le Comité européen pour les problèmes criminels (CDPC) a présenté le 5 mai 2021 un avis sur le projet de 2e protocole additionnel qui avait été préparé par le PC-OC[2] et approuvé par le CDPC.

[2] Comité d'experts sur le fonctionnement des conventions européennes relatives à la coopération dans le domaine pénal (organe subordonné du CDPC).

Dans l'ensemble, le CDPC appuie le projet de protocole et estime qu'il « apportera une réelle valeur ajoutée à la coopération internationale dans le domaine de la cybercriminalité et du recueil de preuves sous forme électronique ».

Le CDPC/PC-OC aurait préféré :

- tout en se félicitant des dispositions relatives à la coopération dans les situations d'urgence, la clarification de la notion de « sécurité d'une personne » dans la définition de « situation d'urgence » ;

- un alignement plus étroit de l'article 11 (vidéoconférence) sur la disposition correspondante du 2e Protocole additionnel à la Convention sur l'entraide judiciaire en matière pénale (STE n° 182), mais constate que, s'agissant des vidéoconférences, le Protocole ne s'appliquera pas aux Parties à la STE 182.

### 3.1.2 Commentaire

- En définissant le terme « situation d'urgence », le projet de Protocole laisse aux Parties une marge de manœuvre concernant la manière de l'appliquer à la sécurité d'une personne physique ; des exemples de telles situations sont présentés dans le Rapport explicatif (voir les paragraphes 41 à 42 du Rapport explicatif).

- Le groupe de rédaction du protocole (T-CY) a bénéficié d'échanges antérieurs avec des membres du PC-OC et a donc été en mesure de préciser la relation entre les dispositions de ce protocole et d'autres traités pertinents, en particulier le STE n° 182, dans le dispositif (voir l'article 5) et le Rapport explicatif (voir, par exemple, les paragraphes 62-67, 69 et 182-186).

## 3.2 Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel (T-PD)

### 3.2.1 Résumé des points soulevés par le T-PD

Donnant suite à une demande du Secrétariat de T-CY, le T-PD a communiqué, le 7 mai 2021, un avis sur le projet de 2e Protocole additionnel.

Le T-PD est convenu que l'article 14 du projet de protocole sur la protection des données à caractère personnel est un compromis obtenu au terme des négociations menées avec un large éventail de pays et de systèmes juridiques, a reconnu le potentiel de telles dispositions autonomes et s'est félicité que sa mise en œuvre soit évaluée au titre de l'article 23. Il reconnaît en outre que l'article 14 ne vise pas à harmoniser les régimes nationaux de protection des données. Dans ce contexte, le T-PD invite les Parties à la Convention de Budapest et à son futur Protocole à adhérer à la Convention 108+ afin de mieux harmoniser les règles relatives à la protection des données à caractère personnel.

S'agissant de l'article 14, le T-PD formule les recommandations suivantes :

- Rappeler l'importance des normes énoncées aux paragraphes 2-15 lorsque les Parties choisissent les options 1.b ou 1.c pour le transfert des données à caractère personnel ;

- Confirmer dans le Rapport explicatif que la Convention 108+ peut être considérée en tant que telle comme un accord visé au paragraphe 1.b ;

- Éviter qu'en vertu de l'option 1.c, les données à caractère personnel soient transférées sans aucune garantie de protection des données ;

- Clarifier davantage, au paragraphe 4, l'expression « considérés comme sensibles compte tenu des risques qu'elles comportent » ;

- Étendre la portée du paragraphe 8 (tenue des registres) pour y inclure le « stockage » et l' « utilisation » ;

- Exiger que, pour les transferts ultérieurs vers un autre État ou vers une organisation internationale (paragraphe 10), l'autorité de transfert tienne dûment compte d'un niveau de protection approprié conformément à l'article 14.

En ce qui concerne les articles 7 et 8, le T-PD propose que le Protocole précise « le moment où un prestataire de services sera considéré comme 'physiquement présent' sur le territoire d'une Partie ».

En ce qui concerne l'article 8, le T-PD propose d'appliquer à la divulgation des données de trafic la protection combinée des données et d'autres garanties de la Partie requérante, de la Partie où la personne concernée était présente lors de l'utilisation du service ciblé, et de la Partie où est implanté le fournisseur de services.

En ce qui concerne les articles 6 et 7, le T-PD propose des exigences de « confidentialité stricte » pour les prestataires, comme prévu à l'article 9.

### 3.2.2 Commentaire

- L'option 1.b prévue à l'article 14 ne s'applique qu'aux accords internationaux établissant un cadre global pour la protection des données à caractère personnel, applicable au transfert de ces données à des fins de prévention, de détection, d'investigation et de poursuite d'infractions pénales, et qui prévoient que le traitement des données à caractère personnel effectué en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées. Par conséquent, sur le plan pratique, les dispositions de ces accords (il s'agit probablement de la Convention 108+ pour de nombreuses Parties) sont susceptibles d'être similaires, voire plus complètes et plus spécifiques que celles énoncées aux paragraphes 2 à 15 de l'article 14.

- Le paragraphe 224 du Rapport explicatif fait spécifiquement référence à la Convention 108+ en tant qu'accord applicable en vertu de l'option 1.b. Les dispositions de la Convention 108+ s'appliqueraient dans les relations entre les Parties à ladite convention, pour les mesures relevant du champ d'application de cet accord, aux données à caractère personnel reçues en vertu du protocole en lieu et place des paragraphes 2 à 15 de l'article 14.

- L'option 1.c ne s'appliquerait qu'entre les Parties dont les accords ou arrangements autorisent l'application de normes différentes ; à cet égard, certaines délégations ont fait référence à des accords d'entraide existants.

- Le paragraphe 4 de l'article 14 couvre les « données sensibles ». Le paragraphe 237 du Rapport explicatif explique que « si certaines formes de données biométriques peuvent être jugées sensibles au vu des risques qu'elles impliquent, ce n'est pas le cas de toutes». Étant donné que le degré de sensibilité des données biométriques peut varier, les Parties bénéficient d'une certaine souplesse dans la réglementation de ce domaine. Certains des concepts utilisés dans la Convention 108+ (y compris l'expression « résultant d'un traitement technique spécifique » au paragraphe 58 du Rapport explicatif de la Convention 108+) peuvent également être interprétés différemment dans différentes Parties à cette Convention. Suite à l'avis du T-PD, les précisions suivantes ont été ajoutées au paragraphe 239 du Rapport explicatif du Protocole : « En ce qui concerne les Parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), telle qu'amendée par le Protocole (STE n° 223), l'interprétation de ce qui constitue des données biométriques « sensibles » devrait être guidée par l'article 6, paragraphe 1, de cette Convention, tel que détaillé aux paragraphes 58 et 59 de son Rapport explicatif. »

- L'article 14, paragraphe 8, inclut les termes « utilisé » et « accédé » ; l'intérêt d'ajouter le terme « stocké » n'est pas manifeste.

- En ce qui concerne l'article 14, paragraphe 10, le paragraphe 265 du Rapport explicatif traite du point soulevé par le T-PD.

- La définition du moment où un prestataire de services est considéré comme « physiquement présent » peut varier d'un système juridique à l'autre et peut également évoluer ; malgré ces restrictions, les rédacteurs ont apporté des précisions concernant les paragraphes 99 et 128 du Rapport explicatif.

- La faisabilité de l'application éventuelle des garanties combinées de protection des données de la Partie requérante, de la Partie du prestataire de services et de la Partie où la personne concernée était présente lors de l'utilisation du service ciblé sans efforts déraisonnables n'est pas claire car l'identité et la localisation d'une personne ne sont généralement pas connus au début d'une enquête. Elle peut également nécessiter des enquêtes supplémentaires pour repérer le lieu de résidence d'un utilisateur. Enfin, une telle approche alourdit les charges au-delà de ce qui est même nécessaire dans le cadre des régimes d'entraide judiciaire.

- Les dispositions relatives à la coopération directe constituent une base permettant aux Parties requérantes de fournir des instructions procédurales spéciales afin de rechercher la confidentialité dans la mesure du possible, par exemple, sous réserve des exigences du droit national. Dans certains États parties, la confidentialité de l'injonction est maintenue de plein droit, alors que ce n'est pas nécessairement le cas dans d'autres États parties (voir les paragraphes 84.d et 106 du rapport explicatif).

# 4 Soumissions d'autres parties prenantes

## 4.1 Commentaires sur les soumissions relatives au chapitre II (Mesures de coopération renforcée)

### 4.1.1 Le protocole ne doit pas abaisser le niveau des normes

- Les craintes que le Protocole abaisse le niveau des normes et des protections ne sont pas justifiées. Comme tout traité multilatéral, le présent Protocole doit tenir compte du fait que les Parties ont des systèmes juridiques différents et, partant, des systèmes de protection différents. Le Protocole prévoit des réserves, des déclarations et d'autres dispositions pour tenir compte des normes et protections des Parties et veiller à ce qu'elles ne soient pas affaiblies (par exemple, les déclarations figurant au paragraphe 2 b) de l'article 7 et au paragraphe 5 de l'article 7).

- Le Protocole crée un cadre clair assorti de conditions et de garanties. En outre, contrairement à d'autres instruments internationaux sur la coopération en matière pénale, le Protocole comprend un article très détaillé sur la protection des données à caractère personnel transférées en vertu dudit protocole.

### 4.1.2 L'entraide devrait être privilégiée par rapport aux demandes ou injonctions directes

- L'entraide judiciaire est, et restera probablement, le principal moyen de recueillir un large éventail de preuves auprès d'autres juridictions aux fins d'une procédure pénale. Après des analyses détaillées, le T-CY a adopté en 2014 une série de recommandations visant à rendre plus efficace l'entraide judiciaire en matière de cybercriminalité et de recueil de preuves électroniques. Ces recommandations ont été suivies par les Parties à la Convention de Budapest, le T-CY et dans le cadre de projets de renforcement des capacités ; des mesures de type entraide judiciaire ont également été incluses dans ce Protocole (articles 10, 11 et 12).

- Toutefois, le T-CY a également conclu que, pour certains types d'informations ou dans certaines circonstances, d'autres moyens de coopération doivent être mis à disposition. Il s'agit en particulier des informations sur les abonnés et des informations sur l'enregistrement des noms de domaine. Si les demandes ou injonctions relatives à de telles informations peuvent être traitées par le biais d'une coopération directe, les systèmes d'entraide judiciaire disposeraient de davantage de ressources pour des demandes et affaires plus complexes nécessitant des mesures plus intrusives.

### 4.1.3 Approbation judiciaire ou autre approbation indépendante obligatoire des demandes ou des injonctions

- Les Parties à la Convention de Budapest ont diverses exigences pour obtenir différents types de données. Selon leur système juridique interne, les éléments de preuve peuvent être sollicités ou autorisés par les procureurs, les grands jurys, les juges d'instruction, les juges ou d'autres autorités. Étant donné les différents régimes en vigueur dans les Parties, il a été jugé disproportionné d'exiger une autorisation judiciaire dans tous les cas de figure. Certaines Parties ayant besoin de disposer d'une garantie supplémentaire permettant un contrôle plus poussé de la légalité de l'injonction, le paragraphe 2 b) de l'article 7 autorise les Parties à faire une déclaration indiquant que « l'injonction adressée

en application [du paragraphe 1] doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une forme de supervision indépendante » (voir également le paragraphe 101 du Rapport explicatif du Protocole).

- Il a été jugé disproportionné d'exiger une autorisation judiciaire pour les demandes d'informations relatives à l'enregistrement de noms de domaine au titre de l'article 6, étant donné que la disposition (au paragraphe 1) ne fournit qu'une base pour les demandes et (au paragraphe 2) exige des Parties qu'elles veillent à ce que ces entités soient autorisées à divulguer les données demandées. En outre, les données d'enregistrement comprennent des informations de base qui ne peuvent être considérées que comme un sous-ensemble limité de données relatives aux abonnés et ne permettent pas de tirer des conclusions précises concernant la vie privée et les habitudes quotidiennes des individus (voir les paragraphes 80 et 82 du Rapport explicatif). En outre, les demandes se limitent à des enquêtes ou procédures pénales spécifiques ; la divulgation est soumise à des conditions raisonnables prévues par le droit interne ; et les garanties des articles 13 et 14 s'appliquent.

- Tous les systèmes juridiques n'exigent pas un contrôle juridictionnel *ex ante* des mesures prévues par le présent Protocole, mais ils autorisent l'implication ultérieure des juges dans les procédures. Il ne serait pas possible d'imposer un modèle unique étant donné le grand nombre de Parties à la Convention.

### 4.1.4 Notification obligatoire aux autorités, aux États requis ou aux États de résidence

- Si certaines Parties ont estimé qu'il est nécessaire de recevoir une notification lorsqu'une autre Partie adresse une injonction de produire des informations sur les abonnés à un fournisseur situé sur leur territoire en vertu de l'article 7, dans chaque cas ou dans certaines circonstances déterminées, d'autres ont craint que leurs autorités centrales ne soient submergées par un grand nombre de notifications ou que cela ne soit pas nécessaire dans toutes les situations. Afin de répondre à ces exigences et préoccupations, les Parties ont eu la possibilité d'exiger une notification conformément au paragraphe 5 de l'article 7.

- Comme indiqué plus haut à propos des commentaires du T-PD, la notification de l'État de résidence pose un certain nombre de difficultés aux États (et pas uniquement à l'État du prestataire de services) car elle pourrait créer une charge disproportionnée pour les autorités chargées de l'enquête, qui seraient obligées d'ouvrir une enquête supplémentaire pour déterminer le lieu de résidence, et ajouter ainsi une condition qui n'entre pas, normalement, dans le cadre de l'entraide judiciaire.

### 4.1.5 Notification obligatoire à la personne dont les données sont demandées

- Les lois nationales des Parties varient en ce qui concerne la possibilité et le moment où les sujets peuvent ou doivent être notifiés dans le cadre d'une enquête pénale. La question de la notification et des limitations de cette notification est traitée au paragraphe 11 de l'article 14.

### 4.1.6 Autoriser les entités du secteur privé à consulter les autorités au sujet d'une demande et/ou de s'y opposer

- Les articles 6 et 7 sont conçus de manière à éviter les échanges réciproques en précisant quelles informations doivent être fournies dans les demandes et les injonctions. En vertu du paragraphe 5 b) de l'article 7, une Partie peut exiger d'un prestataire de services situé sur son territoire qu'il consulte ses autorités dans certaines circonstances déterminées (voir également le paragraphe 108 du Rapport explicatif).

### 4.1.7 Création de mécanismes publics de contrôle, de transparence et de statistiques

- Les propositions selon lesquelles les demandes transfrontalières, notamment la divulgation d'informations en cas d'urgence (article 9), doivent être soumises à un mécanisme de contrôle public, ne seraient pas compatibles avec les principes de l'État de droit dans la mesure où de tels organes de contrôle superviseraient le système de justice pénale. Les autorités de justice pénale sont étroitement réglementées et soumises à un contrôle à tous les stades. Cela vaut également pour les équipes communes d'enquête (article 12), qui font l'objet d'un contrôle, et les actions coercitives dans chaque partie participante peuvent nécessiter une autorisation judiciaire.

- La collecte de statistiques annuelles sur les demandes adressées aux prestataires de services pourrait être l'une des tâches du T-CY dans le cadre du suivi de la mise en œuvre du protocole par les Parties. En fait, le T-CY, dans ses travaux préparatoires au Protocole (Groupe sur les preuves dans le nuage, T-CY), avait largement utilisé les données publiées par les prestataires de services dans leurs rapports sur la transparence. Or l'intention n'était pas d'obliger les prestataires de services à publier de tels rapports. À la suite des consultations, le paragraphe 106 du Rapport explicatif a été révisé afin de préciser qu'une « demande de confidentialité ne devrait pas empêcher les prestataires de services de rendre compte, dans un souci de transparence, des nombres agrégés anonymes d'injonctions reçues au titre du présent article ».

### 4.1.8 Article 6 (Demande d'informations concernant l'enregistrement d'un nom de domaine)

- En ce qui concerne la question de savoir si l'article 6 s'applique aux entités fournissant des services d'enregistrement de noms de domaine ou à toute « entité fournissant des services d'enregistrement de noms de domaine », y compris les services de résolution de noms de domaine, les revendeurs ou les fournisseurs de proxy privé, c'est le premier cas (voir l'article 6, paragraphe 1, qui fait désormais référence à une demande « à émettre auprès d'une entité fournissant des services d'enregistrement de noms de domaine »).

- Quant à la proposition selon laquelle le paragraphe 2 de l'article 6 permet à une entité de divulguer des informations « sous réserve des conditions raisonnables prévues par le droit interne », le paragraphe 2 prévoit que la divulgation est permise « sous réserve des conditions raisonnables prévues par la loi nationale », et le paragraphe 82 du Rapport explicatif précise que « dans certaines Parties [cela] peut inclure des conditions découlant des lois sur la protection des données à caractère personnel ».

- L'article 6 est soumis aux articles 13 et 14 du Protocole.

- L'obligation de notifier l'État de l'entité au moment de l'envoi des demandes a été jugée inutile compte tenu de la nature de ces informations et du fait que cette disposition devrait compléter les politiques multipartites pertinentes en matière de gouvernance de l'internet (paragraphe 76 du rapport explicatif). L'obligation de notification irait à l'encontre de ces politiques et pratiques.

- L'article 6 est une mesure spécifique aux informations relatives à l'enregistrement des noms de domaine et est moins complexe que l'article 7. Selon les circonstances et le droit interne, une entité fournissant des services d'enregistrement de noms de domaine peut également être considérée comme un prestataire de services et les informations relatives à l'enregistrement de noms de domaine peuvent également être considérées (comme un sous-ensemble) d'informations sur les abonnés. Il n'est donc pas exclu que, dans de telles situations, l'article 7 soit utilisé pour obtenir la divulgation d'informations relatives à l'enregistrement de noms de domaine.

### 4.1.9 Article 7 (Divulgation directe de données relatives aux abonnés)

- En ce qui concerne la proposition visant à préciser le terme « données relatives aux abonnés » et à exclure les données relatives au trafic, les paragraphes 92 et 93 du Rapport explicatif fournissent déjà une précision à ce sujet. En outre, les Parties peuvent invoquer le paragraphe 9 b) de l'article 7 pour ne pas appliquer ledit article à certains types de numéros d'accès si cela est incompatible avec les principes fondamentaux de leur système juridique interne.

- En ce qui concerne le respect du privilège lié au secret professionnel de l'avocat et à des privilèges similaires, cette disposition permet aux Parties qui choisissent de recevoir des notifications d'invoquer des motifs de refus prévus dans les traités d'entraide judiciaire ou les lois nationales applicables et offre « des garanties pour les droits des personnes se trouvant dans la Partie requise » (clarification ajoutée au paragraphe 141 du Rapport explicatif à la suite des consultations). En tout état de cause, l'article 7 ne concerne que les informations relatives aux abonnés et non, par exemple, les communications privilégiées entre les avocats et leurs clients.

- Quant à la proposition d'élaborer des modèles pour les demandes adressées aux prestataires de services, elle pourrait être reprise par le T-CY (comme cela a été fait précédemment pour la Convention) afin de faciliter la coopération, comme cela a été fait précédemment pour les demandes de préservation et d'entraide judiciaire.

### 4.1.10 Article 12 (Equipes communes d'enquête et enquêtes communes)

- Lorsque des mesures sont exécutées dans une Partie participant à une équipe commune d'enquête, les autorités de cette Partie déterminent si elles peuvent effectuer la mesure d'enquête en question en fonction de son droit interne.

- Il a été également expliqué plus haut que les équipes communes d'enquête sont soumises aux mécanismes de contrôle du système de justice pénale.

- La publication des termes d'un accord relatif à l'équipe commune d'enquête peut enfreindre les règlements concernant le secret des enquêtes ou même les droits des personnes faisant l'objet d'une enquête.

## 4.2 Commentaires sur les observations relatives au chapitre III (Conditions et garanties)

### 4.2.1 Commentaire général

- Les mesures du Protocole sont soumises à de multiples conditions et garanties qui s'ajoutent à celles des articles 13 et 14, par exemple :

  - les mesures prévues par le Protocole ne s'appliquent qu'aux enquêtes et procédures pénales spécifiques ;
  - Les Parties doivent adopter « les mesures législatives ou autres pouvant se révéler nécessaires pour s'acquitter des obligations entérinées dans le présent Protocole » dans leur droit interne (voir la règle générale à l'article 2, paragraphe 2 ; et ses itérations, par exemple, à l'article 6, paragraphe 2, ou à l'article 7, paragraphe 2) ;
  - les articles énumèrent les injonctions ou demandes à spécifier et les informations complémentaires à fournir (voir par exemple l'article 7, paragraphes 3 et 4) ;
  - les réserves et déclarations permettent aux Parties de satisfaire à des exigences spécifiques de leur droit interne (par exemple, le régime de notification prévu au paragraphe 5 de l'article 7) ;
  - des restrictions d'utilisation, des exigences de confidentialité ou des motifs de refus peuvent s'appliquer.

- Et surtout, les mesures du Protocole seront intégrées dans le système de justice pénale d'une Partie et chaque Partie sera tenue de veiller à ce que l'établissement, la mise en œuvre et l'application des pouvoirs prévus dans le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui assurera une protection adéquate des droits de l'homme et des libertés (article 13 ; voir également l'article 15 de la Convention).

- En ce qui concerne la proposition de mettre les mesures prévues par le Protocole à disposition pour obtenir des informations ou des éléments de preuve aux fins de la défense d'un accusé (ce que certains commentateurs ont qualifiée d' « égalité des armes »), cette question n'est pas régie par la Convention sur la cybercriminalité. Elle est plutôt soumise au droit interne d'une Partie et il ne serait donc pas possible d'établir une règle générale à cet égard dans le présent Protocole.

### 4.2.2 Article 13 (Conditions et garanties)

- L'article 13 adapte l'article 15 de la Convention aux mesures prévues par le Protocole. L'article 13 dispose que, « conformément à l'article 15 de la Convention, chaque Partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui doit assurer la protection adéquate des droits de l'homme et des libertés ». L'article 15 de la Convention dispose que « [c]haque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés … et qui doit intégrer le principe de la proportionnalité ». À l'instar du paragraphe 146 du Rapport explicatif à la Convention, le paragraphe 218 de ce Rapport

explicatif au Protocole dispose que le principe de proportionnalité « est mis en œuvre par chaque Partie conformément aux principes pertinents de son droit interne ».

### 4.2.3 Article 14 (Protection des données à caractère personnel)

Note: Au moment des consultations, le Rapport explicatif au Protocole concernant l'article 14 n'était pas encore disponible. Entre-temps, un certain nombre de propositions et de questions soulevées par les parties prenantes ont été abordées dans le Rapport explicatif.

- Un grand nombre de Parties à la Convention de Budapest sont également Parties à la Convention 108 du Conseil de l'Europe, lequel a aidé les pays à harmoniser leurs réglementations en matière de protection des données avec la Convention 108 afin de faciliter leur adhésion à cette convention. La Convention 108+ n'est pas encore entrée en vigueur, mais le Conseil de l'Europe suit une approche similaire en ce qui la concerne. Cependant, l'adhésion à la Convention 108 ou à la Convention 108+ ne saurait être une condition pour devenir Partie à la Convention de Budapest ou à ses Protocoles. L'article 14, paragraphe 1.b, prévoit que, entre les Parties à cette Convention, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application du présent Protocole, aux données à caractère personnel reçues en vertu du Protocole en lieu et place des paragraphes 2 à 15.

- Le Protocole, dans son article 14, prévoit des exigences fondamentales en matière de protection des donnée, qui s'appliquent, notamment, aux éléments suivants : « but et utilisation », « qualité et intégrité », « tenue de registres », « sécurité des données et incidents de sécurité », « accès et rectification » et « recours judiciaire et non judiciaire ».

- L'article 14 exige également un « contrôle indépendant et effectif » conformément aux dispositions du paragraphe 14. Or certains ont suggéré qu'il ne serait pas compatible avec les principes de l'état de droit que ces organes de contrôle aient la compétence de superviser le système de justice pénale, par exemple en contrôlant les injonctions ou les demandes.

- En ce qui concerne la suggestion selon laquelle les Parties peuvent imposer unilatéralement à tout moment des exigences supplémentaires en matière de protection des données, il semble qu'elle irait à l'encontre de l'objectif de l'article 14 consistant à fournir une base pour les transferts internationaux de données à caractère personnel en prévoyant des garanties appropriées. Comme expliqué au paragraphe 224 du Rapport explicatif, le paragraphe 1.d de l'article 14 est donc « producteur de sécurité juridique pour les transferts internationaux de données à caractère personnel effectués en vertu des paragraphes 1.a ou 1.b en réponse aux injonctions ou demandes adressées en vertu du présent Protocole, le but étant de garantir l'efficacité et la prévisibilité des échanges de données ». Et le paragraphe 225 du Rapport explicatif explique qu'en outre, « le paragraphe 1.d dispose qu'une Partie est autorisée à refuser ou à empêcher les transferts de données à une autre Partie en vertu du présent Protocole uniquement pour des raisons de protection des données : i) dans les conditions exposées au paragraphe 15 relatif à la consultation et à la suspension ou ii) aux termes d'accords ou d'arrangements spécifiques visés aux paragraphes 1.b ou 1.c, lorsque l'un de ces paragraphes s'applique. »

- En ce qui concerne le traitement des données dans un « but légitime », le paragraphe 2 de l'article 14 (but et utilisation) indique clairement que la « Partie destinataire de

données à caractère personnel traite lesdites données aux fins prévues à l'article 2 » du Protocole. L'article 2 définit le « champ d'application » du Protocole, à savoir qu'il s'applique « à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des systèmes et des données informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique » (voir également les paragraphes 227 à 231 du Rapport explicatif). En outre, selon le paragraphe 227 du Rapport explicatif, il faut que « les autorités aient ouvert une enquête ou entamé des poursuites concernant une activité criminelle définie, cette enquête ou ces poursuites constituant le but légitime dans lequel il est possible d'obtenir des preuves ou des informations contenant des données à caractère personnel et de les traiter ».

- Il est rappelé que « [c]haque Partie adopte les mesures législatives ou autres pouvant se révéler nécessaires pour s'acquitter des obligations entérinées dans le présent Protocole ». (voir le paragraphe 2 de l'article 2; voir également le paragraphe 2 de l'article 6 et le paragraphe 2 de l'article 7).

- Les « durées de conservation » sont visées par le paragraphe 5 de l'article 14 et expliquées plus en détail aux paragraphes 240 à 242 du rapport explicatif. La « tenue de registres » est couverte par le paragraphe 8 de l'article 14 et est expliquée plus en détail aux paragraphes 257 à 258 du Rapport explicatif. Les systèmes de justice pénale ont généralement des règles détaillées pour les durées de rétention, mais ces périodes peuvent différer d'une Partie à l'autre. Il convient donc d'accorder une marge d'appréciation quant à la manière dont les Parties les réglementent en détail.

- Quant à la suggestion relative au paragraphe 11.a de l'article 14, selon laquelle la référence à la manière dont les notifications générales sont assurées manque de précision concernant la mise en œuvre, et que cela pourrait être traité en faisant référence à un « site internet gouvernemental ou à d'autres médias accessibles au public », elle a été prise en compte et précisée au paragraphe 267 du rapport explicatif.

- En ce qui concerne la proposition d'indiquer à l'article 12 qu'une personne peut recevoir une confirmation du traitement, il est bon de noter qu'une explication supplémentaire a été insérée au paragraphe 271 du rapport explicatif, selon laquelle cette disposition « peut également permettre à l'individu de confirmer si (ou non) ses données personnelles ont été obtenues en vertu du Protocole, et ont été ou sont traitées » (clarification ajoutée à la suite des consultations).

- S'agissant des restrictions au droit d'accès en vertu du paragraphe 12 de l'article 14, le paragraphe 272 du rapport explicatif précise désormais également que « les restrictions proportionnées doivent protéger les droits et libertés d'autrui ou protéger des objectifs importants d'intérêt public général et tenir dûment compte des 'intérêts légitimes de la personne concernée' ». L'expression « 'intérêts légitimes de la personne concernée' a été considérée par les rédacteurs comme incluant les droits et libertés de la personne ».

- En ce qui concerne les propositions relatives à la « surveillance » (paragraphe 14 de l'article 14), le dispositif a été modifié pour inclure « le pouvoir de donner suite aux plaintes », et le paragraphe 281 du Rapport explicatif a été modifié et prévoit désormais que « [d]es consultations entre les autorités respectives des Parties dans l'exercice de leurs fonctions de surveillance en vertu du présent article peuvent avoir lieu, le cas échéant. »

- Quant à la suggestion selon laquelle, dans les situations de partage ultérieur (paragraphe 9 de l'article 14), l'autorité de transfert devrait être informée du partage ultérieur et du traitement ultérieur envisagés, les Parties ont estimé que la valeur ajoutée de ces informations n'est pas manifeste compte tenu des garanties déjà incluses dans le Protocole, en particulier à l'article 14 sur la protection des données.

- En ce qui concerne la participation d'experts de la protection des données aux évaluations effectuées en application de l'article 23 du Protocole, une phrase supplémentaire a été ajoutée au paragraphe 322 du Rapport explicatif, indiquant que « [c]ompte tenu de l'expertise nécessaire à l'évaluation de l'utilisation et de la mise en œuvre de certaines dispositions du présent Protocole, notamment de l'article 14 sur la protection des données, les Parties peuvent envisager d'associer leurs experts en la matière aux évaluations ». Peuvent être inclus, par exemple, des représentants des autorités chargées de la protection des données.

# 5 Conclusion

Cette sixième série de consultations – comme les précédentes – a contribué à l'élaboration du projet de protocole. À la suite de la réunion du 6 mai 2021 et de l'examen des soumissions écrites, un certain nombre de modifications ont été apportées à ce projet.

S’agissant des autres propositions et demandes de renseignements, les commentaires informels qui sont exposés dans le présent résumé concernent les contributions, demandes de renseignements et propositions faites par des intervenants, mais il est indiqué plus haut qu’ils ne reflètent pas nécessairement les avis des rédacteurs du Protocole, lesquels sont exposés dans le Rapport explicatif du Protocole.

Ce Protocole est un instrument complexe et le résultat de négociations approfondies entre un grand nombre de pays dotés de divers systèmes juridiques. Plus de quatre-vingt-dix réunions ont été nécessaires pendant près de quatre ans pour parvenir à ce projet de protocole qui concilie les mesures permettant d’apporter une réponse effective de la justice pénale avec un État de droit fort et des garanties solides en matière de protection des données.

# 6 Annexe

## 6.1 Ordre du jour des consultations du 6 mai 2021

### Comité de la Convention cybercriminalité (T-CY)

**Préparation d'un 2e Protocole additionnel à la Convention de Budapest sur la cybercriminalité**

## 6e série de consultations avec les parties prenantes

**Réunion en ligne, 12 heures – 18 heures (France), 6 mai 2021**

| | |
|---|---|
| **12 heures -14 h 30** | **Partie 1 : Vue d'ensemble et examen du chapitre II** |
| | Observations liminaires |
| | Aperçu du projet de Protocole |
| | Chapitre II : Résumé des soumissions écrites[3]. |
| | Débat |
| 14 h 30-16 heures | Pause |
| **16 heures - 18 heures** | **Partie 2 : Conditions et garanties** |
| | Aperçu des conditions et garanties prévues par le Protocole |
| | Présentation de l'article 14 sur la protection des données |
| | Débat |

[3] Pour les soumissions écrites et le projet de texte du Protocole, voir : Consultations sur le protocole (coe.int)

## 6.2 Liste des participants

**Comité de la Convention sur la cybercriminalité, T-CY**
**Préparation d'un 2e Protocole additionnel à la Convention de Budapest sur la Cybercriminalité**
**6e série de consultations avec les parties prenantes – 6 mai 2021**

**COUNTRIES / *PAYS***

| | |
|---|---|
| ARGENTINA / *ARGENTINE* | Dominique PAZ<br>Cybercrime Prosecutor Office / *Bureau du procureur chargé de la cybercriminalité* |
| ARGENTINA / *ARGENTINE* | Aldana ROHR<br>Ministry of Foreign Affairs / *Ministère des affaires étrangères* |
| ARGENTINA / *ARGENTINE* | Agustina SIRVEN<br>AAIP / *AAIP* |
| ARGENTINA / *ARGENTINE* | Mauro MELONI<br>Personal Data Protection National Agency / *Agence nationale de protection des données personnelles* |
| ARGENTINA / *ARGENTINE* | Eduardo CIMATO<br>Personal Data Protection National Agency / *Agence nationale de protection des données personnelles* |
| ARGENTINA / *ARGENTINE* | Cecilia GARIBOTTI<br>Personal Data Protection National Agency / *Agence nationale de protection des données personnelles* |
| AUSTRALIA / *AUSTRALIE* | Nathan WHITEMAN<br>Department of Home Affairs / *Département des affaires intérieures* |
| AUSTRALIA / *AUSTRALIE* | Emily HITCHMAN<br>Department of Home Affairs / *Département des affaires intérieures* |
| BELGIUM / *BELGIQUE* | Delphine WYNANTS<br>Federal Public Service Justice / *Service Public Fédéral Justice* |
| CANADA / *CANADA* | Normand WONG<br>Ministry of Justice / *Ministère de la Justice* |
| CANADA / *CANADA* | Tom BEVERIDGE<br>Counsellor, International Criminal Operations Mission of Canada to the EU / *Conseiller, Mission d'opérations criminelles internationales du Canada auprès de l'UE* |
| CANADA / *CANADA* | Philip LUPUL<br>Criminal, Security, Diplomatic Law Division / *Division du droit pénal, de la sécurité et du droit diplomatique* |

| | |
|---|---|
| CANADA / *CANADA* | Gareth SANSOM<br>Federal Department of Justice / *Département fédéral de la justice* |
| CANADA / *CANADA* | Jacqueline PALUMBO<br>Ministry of Justice / *Ministère de la Justice* |
| CANADA / *CANADA* | Anne-Marie LE BEL<br>Ministry of Justice / *Ministère de la Justice* |
| CANADA / *CANADA* | Tebello MOROJELE<br>Global Affairs / *Affaires mondiales* |
| CANADA / *CANADA* | Ian DOUGLAS<br>Office of the Privacy Commissioner of Canada / *Commissariat à la protection de la vie privée du Canada* |
| COLOMBIE /*COLOMBIE* | Jefferson Rolando ROJAS RODRIGUEZ<br>Attorney's General Office / *Bureau du procureur général* |
| COLOMBIA / *COLOMBIE* | Juan Pablo SALAZAR HOYOS<br>Ministry of Information and Communication Tehcnologies / *Ministère des technologies de l'information et de la communication* |
| COLOMBIA / *COLOMBIE* | Diana Carolina KECAN CERVANTES<br>Ministry of Foreign Affairs / *Ministère des affaires étrangères* |
| COLOMBIA / *COLOMBIE* | Jehudi CASTRO<br>Presidency of the Republic / *Présidence de la République* |
| CROATIA / *CROATIE* | Zrinka SALAJ<br>Ministry of Foreign Affairs / *Ministère des affaires étrangères*<br>Permanent Representation of Croatia to the European Union / *Représentation permanente de la Croatie auprès de l'Union européenne* |
| CZECH REPUBLIC / *RÉPUBLIQUE TCHÈQUE* | Jakub PASTUSZEK<br>Ministry of Justice / *Ministère de la Justice* |
| DOMINICAN REPUBLIC / *RÉPUBLIQUE DOMINICAINE* | Cesar MOLINE RODRIGUEZ<br>Institute for Telecommunications */ Institut des télécommunications* |
| ESTONIA / *ESTONIE* | Markko KÜNNAPU<br>Ministry of Justice / *Ministère de la Justice* |
| FINLAND / *FINLANDE* | Janne KANERVA<br>Ministry of Justice / *Ministère de la Justice* |
| FRANCE / *FRANCE* | Caroline BOTSCHI<br>Ministry of Justice / *Ministère de la Justice* |
| FRANCE / *FRANCE* | Etienne MAURY<br>CNIL / *Conseiller juridique et CNIL* |

| | |
|---|---|
| GERMANY / *ALLEMAGNE* | Sara CLAASSEN<br>Federal Ministry of Justice and Consumer Protection / *Ministère fédéral de la justice et de la protection des consommateurs* |
| GERMANY / *ALLEMAGNE* | Lisa BÜTTGEN<br>German DPA (BfDI, Federal Commissioner for Data Protection and Freedom of Information) / Autorité allemande de protection des données (BfDI, Commissaire fédéral à la protection des données et à la liberté d'information) |
| GERMANY / *ALLEMAGNE* | Frederic BARTH<br>Federal Ministry of Justice and Consumer Protection / *Ministère fédéral de la justice et de la protection des consommateurs* |
| JAPAN / *JAPON* | Satoshi YANAGISAWA<br>Ministry of Foreign Affairs/ *Ministère des affaires étrangères* |
| JAPAN / *JAPON* | Hideaki KOJIMA<br>Consulate General of Japan in Strasbourg / *Consulat général du Japon à Strasbourg* |
| JAPAN / *JAPON* | Kazunori SONOHARA<br>National Police Agency / *Agence nationale de la police* |
| LATVIA / *LETTONIE* | Kristina TIMOFEJEVA<br>National Police / *Police nationale* |
| LATVIA / *LETTONIE* | Olegs OLINS<br>State Police of Latvia / *Police d'État de Lettonie* |
| NORWAY / *NORVÈGE* | Eirik Trønnes HANSEN<br>Prosecutor / *Procureur* |
| NORWAY / *NORVÈGE* | Catharina LURÅS<br>Ministry of Justice and Public Security / *Ministère de la Justice et de la sécurité publique* |
| PORTUGAL / *PORTUGAL* | Maria-José CASTELLO-BRANCO<br>Ministry of Justice / *Ministère de la Justice* |
| PORTUGAL / *PORTUGAL* | Pedro VERDELHO<br>T-CY Vice-Chair / *T-CY Vice-Président*<br>Public Prosecutor / *Procureur général*<br>General Prosecutor's Office of Lisbon / *Bureau du procureur général de Lisbonne* |
| REPUBLIC OF KOREA / *CORÉE DU SUD* | Min Goo Kim<br>Korean National Police Agency / *Agence de la Police Nationale* |
| REPUBLIC OF KOREA / *CORÉE DU SUD* | Seung CHOI<br>KSPO (Korean Supreme Prosecutor's Office)<br>/ *KSPO (Bureau du procureur suprême de Corée)* |
| REPUBLIC OF KOREA / *CORÉE DU SUD* | Representative / Représentant.e<br>National Police / *Police nationale* |

| | |
|---|---|
| ROMANIA / *ROUMANIE* | Cristina SCHULMANN<br>T-CY Chair / *T-CY Présidente*<br>Department for International Law and Judicial Cooperation / *Département pour le droit international et la coopération judiciaire*<br>Ministry of Justice / *Ministère de la Justice* |
| SERBIA / *SERBIE* | Branko STAMENKOVIC<br>Public Prosecutor's Office / *Bureau du procureur* |
| SLOVAKIA / *SLOVAQUIE* | Branislav BOHACIK<br>Republic Prosecutor's Office / *Bureau du procureur de la République* |
| SLOVAKIA / *SLOVAQUIE* | Zuzana ŠTOFOVÁ<br>Ministry of Justice / *Ministère de la Justice* |
| SPAIN / *ESPAGNE* | Maria Elvira TEJADA DE LA FUENTE<br>General Prosecutor's Office / *Bureau du procureur général* |
| SRI LANKA / *SRI LANKA* | Jayantha FERNANDO<br>CERT / *CERT* |
| SRI LANKA / *SRI LANKA* | K.D.G.L Ashoka DHARMASENA<br>Police / *Police* |
| SRI LANKA / *SRI LANKA* | B.V.I GAYASRI<br>Police / *Police* |
| SRI LANKA / *SRI LANKA* | Ravindu MEEGASMULLA<br>CERT / *CERT* |
| SRI LANKA / *SRI LANKA* | Buddhika WIJAYASUNDARA<br>Police / *Police* |
| TURKEY / *TURQUIE* | Gökçen ÇEVİK<br>Ministry of Justice / *Ministère de la Justice* |
| TURKEY / *TURQUIE* | Guray GÜÇLÜ<br>Permanent Representation of Turkey to the CoE/ *Représentation permanente de la Turquie auprès du CoE* |
| UNITED KINGDOM / *ROYAUME UNI* | Representative / Représentant.e<br>Home Office / *Ministère de l'Intérieur* |
| UNITED KINGDOM / *ROYAUME-UNI* | Priya MISTRY<br>Home Office / *Ministère de l'Intérieur* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Benjamin FITZPATRICK<br>Department of State / *Département d'État* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Kenneth HARRIS<br>Senior Counsel for European Union and International Criminal Matters<br>United States Mission to the European Union / *Conseiller principal pour les questions* |

| | |
|---|---|
| | *relatives à l'Union européenne et aux affaires pénales internationales, Mission des États-Unis auprès de l'Union européenne* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Sheri SHEPHERD-PRATT<br>Department of Justice / *Département de la justice* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Katherine HARMAN-STOKES<br>Department of Justice / *Département de la justice* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Erica O'NEIL<br>Department of Justice / *Département de la justice* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Katie EINSPANIER<br>Department of State / *Département d'État* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Hannah MAYER<br>Department of Justice / *Département de la justice* |
| USA / *ÉTATS-UNIS D'AMÉRIQUE* | Benjamin FITZPATRICK<br>Department of State / *Département d'État* |

**ORGANISATIONS**

| | |
|---|---|
| EDPS / *EDPS* | Representative / Représentant.e |
| European data protection supervisor | Niksa STOLIC<br>Legal Officer / *Conseillère juridique* |
| EUROPEAN UNION AGENCY FOR CYBERSECURITY / *AGENCE EUROPÉENNE DE CYBER-SÉCURITÉ* | Silvia PORTESI<br>Cybersecurity Expert / *Expert sécurité* |
| EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE* | Tjabbe BOS<br>DG HOME / *DG Home* |
| EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE* | Manuel GARCIA SANCHEZ<br>(DJ JUST) International data flows and protection / *(DJ JUST) Flux de données et protection au niveau international* |
| EUROPEAN UNION - EUROPEAN COMMISSION / *UNION EUROPEENNE, COMMISION EUROPEENNE* | Gemma CAROLILO<br>Next-generation Internet / *Internet de nouvelle génération* |
| EUROPEAN UNION - EUROPEAN COMMISSION / | Melnia STROUNGI<br>Next-generation Internet / *Internet de nouvelle génération* |

| | |
|---|---|
| *UNION EUROPEENNE, COMMISION EUROPEENNE* | |
| Council of the EU / *Conseil de l'Union européenne* | Leila BEZDROB<br>Trainee / *Stagiaire* |
| Council of the EU / *Conseil de l'Union européenne* | Maria CASTILLEJO<br>Political Administrator / *Administratrice politique* |
| Council of the EU / *Conseil de l'Union européenne* | Christina STROMHOLM<br>Administrator / *Administratrice* |

**ACADEMIA, NON GOVERNMENTAL ORGANISATIONS AND PRIVATE SECTOR / *UNIVERSITES, ORGANISATIONS NON GOUVERNEMENTALES ET SECTEUR PRIVE***

| | | |
|---|---|---|
| Accès immédiat | Estelle MASSE | Senior Policy Analyst / *Analyste politique principale* |
| Accès immédiat | Raman Jit Singh CHIMA | Senior International Counsel and Global Cybersecurity Lead / *Avocat international senior et Responsable de la cybersécurité globale* |
| ADC | Alejo KIGUEL | Analyst / *Analyste* |
| APPLE | Representative / Représentant.e | Privacy Counsel / *Conseiller.e en protection de la vie privée* |
| Binalyze OU | Klaus Peter Finke Härkönen | Strategic Advisor / *Conseiller en stratégie* |
| CCIA | Alexandre ROURE | Senior Manager, Public Policy / *Directeur principal, politique publique* |
| CENTR, | Polina MALAJA | Policy Advisor / *Conseillère en politique* |
| Com Laude Group | Susan PAYNE | Head of Legal Policy / *Cheffe de la section politique juridique* |
| Com Laude Group | Sophie HEY | Policy Advisor / *Conseillère en matière de politique* |
| Council of Bars and Law Societies of Europe (CCBE) | Representative / Représentant.e | |
| Council of Bars and Law Societies of Europe (CCBE) | Martin SACLEUX | Legal advisor / *Conseiller juridique* |
| Council of Bars and Law Societies of Europe (CCBE) | Representative / Représentant.e | |
| Derechos digitales | Maria PAZ CANALES | Executive Director / *Directrice exécutive* |

| | | |
|---|---|---|
| EHFCN | Dimitra LINGRI | Managing Director / *Directrice* |
| Electronic Frontier Foundation | Katitza RODRIGUEZ | Policy Director for Global Privacy / *Directrice de la politique de confidentialité mondiale* |
| EuroISPA | Andreas GRUBER | Chair of the Cybersecurity Committee / *Président du Comité sur la cybersécurité* |
| European Healthcare anti Fraud and Corruption Network | Dimitra LINGRI | Managing Director / *Directrice générale* |
| European Digital Rights | Chloé BERTHÉLÉMY | Policy Advisor / *Conseillère en politique* |
| GOOGLE | Representative / Représentant.e | |
| GOOGLE | Nima BINARA | Counsel / *Conseillère* |
| ICANN | Amy BIVINS | Legal Counsel / *Conseillère juridique* |
| ICANN | Elena PLEXIDA | Vice President Government and IGO Engagement / *Vice-présidente chargée de l'engagement des gouvernements et des OIG* |
| ICANN | Nora MARI | Government and IGO Engagement Manager / *Responsable de l'engagement des gouvernements et des OIG* |
| IT-Pol Denmark | Jesper LUND | Chairman / *Président* |
| Kaspersky | Anastasiya KAZAKOVA | Senior Public Affairs Manager / *Responsable principal des affaires publiques* |
| MARQUES | Clare GRIMLEY | Committee Member, Cyberspace Teal / *Membre du comité, Cyberspace Teal* |
| Reform ICCLR | Jessica JAHN | Associate / *Associée* |
| Sapienza University of Rome | Tommaso PIETRRELLA | PHD Student / *Etudiant en doctorat* |
| University College Dublin Sutherland School of Law | TJ McINTYRE | Associate Professor / *Professeur associé* |
| University of Oxford | Christopher D'URSO | Rhodes Scholar and Dphil (PhD) in Public Policy Student / *Boursier Rhodes et étudiant en Dphil (doctorat) en politique publique* |

| | | |
|---|---|---|
| University of Maryland Global Campus | Felix URIBE | Adjunct Associate Professor / *Professeur associé adjoint* |

**CONSULTANTS / *CONSULTANTS***

| |
|---|
| Betty SHAVE<br>T-CY consultant / *consultante T-CY* |
| MARCOS SALT<br>T-CY consultant / *consultant T-CY* |

**COUNCIL OF EUROPE SECRETARIAT / *SECRETARIAT DU CONSEIL DE L'EUROPE***

| | |
|---|---|
| Patrick PENNINCKX<br>Head of Information Society Department / *Chef du Département de la société de l'Information* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Alexander SEGER<br>Executive Secretary of the Cybercrime Convention Committee / *Secrétaire executif du Comité de la Convention sur la Cybercriminalité* | Head of Cybercrime Division / *Chef de la Division Cybercrime*<br>Head of Cybercrime Programme Office (C-PROC) / Chef du Bureau / *Bureau du programme sur la cybercriminalité (C-PROC)*<br><br>DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Peter KIMPIAN<br>Data Protection Unit / *Unité de Protection des données* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Representative / Représentant.e<br>Moneyval / *Moneyval* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Nina LICHTNER<br>Programme Officer / *Chargée de programme*<br>Cybercrime Division / *Division de la Cybercriminalité* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT - DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Céline DEWAELE<br>Programme Assistante / *Assistante de programme*<br>Cybercrime Division / *Division de la Cybercriminalité* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |

| | |
|---|---|
| Floriane SPIELMANN<br>Project Assistant / *Assistante de projet*<br>Cybercrime Division / *Division de la Cybercriminalité* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |
| Chloé DUMONT<br>*Trainee / Stagiaire* | DIRECTORATE GENERAL HUMAN RIGHTS AND RULE OF LAW – INFORMATION SOCIETY – ACTION AGAINST CRIME DIRECTORATE / *DIRECTION GÉNÉRALE DES DROITS DE L'HOMME ET DE L'ÉTAT DE DROIT – SOCIÉTÉ DE L'INFORMATION – DIRECTION DE L'ACTION CONTRE LE CRIME* |

INTERPRETERS / *INTERPRÈTES*

Chloé CHENETTIER
Sergio Alvarez RUBIO
Hans-Werner MÜHLE
Giamil Ellis LARACUENTE
Stella RAPPOSELLI D'OTTAVIO
Corinne MAGALLON