

CONVENTION SUR LA CYBERCRIMINALITÉ

PROTOCOLE SUR LA XÉNOPHOBIE ET LE RACISME

DEUXIÈME PROTOCOLE SUR LE RENFORCEMENT DE LA COOPÉRATION ET DE LA DIVULGATION DE PREUVES ÉLECTRONIQUES

Rapports explicatifs
et notes d'orientation

www.coe.int/cybercrime

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

CONVENTION SUR LA CYBERCRIMINALITÉ

PROTOCOLE SUR
LA XÉNOPHOBIE
ET LE RACISME

DEUXIÈME PROTOCOLE
SUR LE RENFORCEMENT
DE LA COOPÉRATION
ET DE LA DIVULGATION DE
PREUVES ÉLECTRONIQUES

Rapports explicatifs
et notes d'orientation

Conseil de l'Europe

La reproduction des textes est autorisée à condition d'en citer le titre complet ainsi que la source : Conseil de l'Europe. Pour toute utilisation à des fins commerciales ou dans le cas d'une traduction vers une langue non officielle du Conseil de l'Europe, merci de vous adresser à publishing@coe.int.

Conception de la couverture
et mise en page : Division de
la production des documents
et des publications (DPDP),
Conseil de l'Europe

© Conseil de l'Europe, décembre 2023
Imprimé dans les ateliers
du Conseil de l'Europe

Index

CONVENTION SUR LA CYBERCRIMINALITÉ (STE N° 185) BUDAPEST, 23 NOVEMBRE 2001.	5
Rapport explicatif de la Convention sur la cybercriminalité	37
PROTOCOLE ADDITIONNEL À LA CONVENTION SUR LA CYBERCRIMINALITÉ, RELATIF À L'INCRIMINATION D'ACTES DE NATURE RACISTE ET XÉNOPHOBE COMMIS PAR LE BIAIS DE SYSTÈMES INFORMATIQUES (STE N° 189) STRASBOURG, 28 JANVIER 2003.	145
Rapport explicatif du Premier Protocole additionnel	154
DEUXIÈME PROTOCOLE ADDITIONNEL À LA CONVENTION SUR LA CYBERCRIMINALITÉ RELATIF AU RENFORCEMENT DE LA COOPÉRATION ET DE LA DIVULGATION DE PREUVES ÉLECTRONIQUES (CETS N° 224) STRASBOURG, 12 MAI 2022.	167
Rapport explicatif du Deuxième Protocole additionnel	199
NOTES D'ORIENTATION	311
Note d'orientation sur la notion de « système informatique »	312
Note d'orientation sur les dispositions de la Convention de Budapest visant les botnets	315
Note d'orientation sur les attaques DDOS	319
Note d'orientation sur la fraude par usurpation d'identité et hameçonnage.	322
Note d'orientation sur les attaques visant les infrastructures d'information critiques	328
Note d'orientation sur les nouvelles formes de logiciels malveillants	332
Note d'orientation sur l'accès transfrontalier aux données	336
Note d'orientation sur les spams	344
Note d'orientation sur les injonctions de produire concernant des informations sur les abonnés (Article 18 de la Convention de Budapest)	347
Note d'orientation sur le terrorisme.	357
Note d'orientation sur les aspects de l'ingérence électorale au moyen de systèmes informatiques couverts par la Convention de Budapest	362
Note d'orientation sur les aspects des logiciels rançonneurs couverts par la Convention de Budapest	367
Note d'orientation sur la portée d'application des pouvoirs de procédure et des dispositions portant sur la coopération internationale.	379
Note d'orientation T-CY n° 14 Information spontanée (Article 26 de la Convention sur la cybercriminalité)	388

Convention sur la cybercriminalité (STE n° 185) Budapest, 23 novembre 2001

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention ;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques ;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux ;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information ;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace ;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes

informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable ;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée ;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999) ;

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberspace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8 ;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire

en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information ;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21^e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23^e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité ;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2^e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit :

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

- a. l'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

- b. l'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;
- c. l'expression « fournisseur de services » désigne :
 - i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
 - ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
- d. « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques,

à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.
2. Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :
 - a. la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :
 - i. d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;
 - ii. d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; et

b. la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2. Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3. Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a. par toute introduction, altération, effacement ou suppression de données informatiques ;

- b. par toute forme d'atteinte au fonctionnement d'un système informatique, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie infantine

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit :

- a. la production de pornographie infantine en vue de sa diffusion par le biais d'un système informatique ;
- b. l'offre ou la mise à disposition de pornographie infantine par le biais d'un système informatique ;
- c. la diffusion ou la transmission de pornographie infantine par le biais d'un système informatique ;
- d. le fait de se procurer ou de procurer à autrui de la pornographie infantine par le biais d'un système informatique ;
- e. la possession de pornographie infantine dans un système informatique ou un moyen de stockage de données informatiques.

2. Aux fins du paragraphe 1 ci-dessus, le terme « pornographie infantine » comprend toute matière pornographique représentant de manière visuelle :

- a. un mineur se livrant à un comportement sexuellement explicite ;
- b. une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;
- c. des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3. Aux fins du paragraphe 2 ci-dessus, le terme « mineur » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4. Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.
3. Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne,

toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3. Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

- a. sur un pouvoir de représentation de la personne morale ;
- b. sur une autorité pour prendre des décisions au nom de la personne morale ;
- c. sur une autorité pour exercer un contrôle au sein de la personne morale.

2. Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présente Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3. Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4. Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles

2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2. Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a. aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b. à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c. à la collecte des preuves électroniques de toute infraction pénale.

3. a. Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :

i. qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

- ii. qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1. Chaque 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, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

1. Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a. pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et

b. pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

- a. à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et
 - b. à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.
2. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.
3. Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :
- a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
 - b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
 - c. toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :
- a. à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et
 - b. à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.
2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou

accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

- a. saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;
- b. réaliser et conserver une copie de ces données informatiques ;
- c. préserver l'intégrité des données informatiques stockées pertinentes ;
- d. rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5. Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

- a. à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b. à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

- i. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
- ii. à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habilitier ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

- a. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et
- b. à obliger un fournisseur de services, dans le cadre de ses capacités techniques :
 - i. à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou
 - ii. à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2. Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4. Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

- a. sur son territoire ; ou
- b. à bord d'un navire battant pavillon de cette Partie ; ou
- c. à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou
- d. par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2. Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3. Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4. La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5. Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

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

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1.a. Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b. Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3. Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6. Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7.a. Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.
2. Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.
3. Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.
4. Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.
5. Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1. Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela

pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2. Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

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

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2.a. Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution ;

b. Les autorités centrales communiquent directement les unes avec les autres ;

c. Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe ;

d. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3. Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

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

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

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

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

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

7. La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8. La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9.a. En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b. Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c. Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d. Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e. Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1. En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2. La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande :

a. à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition ; ou

b. à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3. Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4. Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1. Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2. Une demande de conservation faite en application du paragraphe 1 doit préciser :

- a. l'autorité qui demande la conservation ;
- b. l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;
- c. les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;
- d. toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;
- e. la nécessité de la mesure de conservation ; et
- f. le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3. Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4. Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire,

la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5. En outre, une demande de conservation peut être refusée uniquement :

- a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ;
ou
- b. si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6. Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7. Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgence rapide de données conservées

1. Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2. La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

- a. si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou
- b. si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

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.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

- a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou
- b. 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.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1. Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2. Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1. Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

- a. apport de conseils techniques ;
- b. conservation des données, conformément aux articles 29 et 30 ;
- c. recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2.a. Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b. Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou

de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3. Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1. La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2. La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4. Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2. Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1. Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.
2. Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
3. Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1. L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions:
 - de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24) ;
 - de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30) ;
 - du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).
2. Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3. Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1. Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constitutants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2. Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en œuvre des mesures prévues par ledit chapitre.

3. En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constitutants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constitutants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à

l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.
2. Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.
3. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1. Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.
2. Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.
3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.
4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.
5. Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1. Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.
2. En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1. Les Parties se concertent périodiquement, au besoin, afin de faciliter :
 - a. l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention ;
 - b. l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;
 - c. l'examen de l'éventualité de compléter ou d'amender la Convention.
2. Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.
3. Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.
4. Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.
5. Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1. Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.
2. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

- a. toute signature ;
- b. le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;
- c. toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37 ;
- d. toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42 ;
- e. tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

Rapport explicatif de la Convention sur la cybercriminalité

- I. La Convention et son Rapport explicatif ont été adoptés par le Comité des Ministres du Conseil de l'Europe à l'occasion de sa 109^e Session, le 8 novembre

2001. La Convention a été ouverte à la signature à Budapest, le 23 novembre 2001, à l'occasion de la Conférence Internationale sur la Cybercriminalité.

II. Le texte de ce rapport explicatif ne constitue pas un instrument d'interprétation authentique du texte de la Convention, bien qu'il puisse faciliter la compréhension des dispositions qui y sont contenues.

I. Introduction

1. La révolution des technologies de l'information a changé radicalement la société et continuera vraisemblablement de le faire dans un avenir prévisible. Cette révolution a simplifié bien des tâches. Alors qu'initialement, seuls certains secteurs de la société avaient rationalisé leurs méthodes de travail en s'appuyant sur les technologies de l'information, il ne reste pour ainsi dire plus aucun secteur qu'elles n'aient marqué de leur empreinte. Les technologies de l'information se sont insinuées, d'une manière ou d'une autre, dans tous les aspects des activités humaines.

2. Les technologies de l'information se singularisent notamment par l'impact qu'elles ont eu et continueront d'avoir sur l'évolution des technologies des télécommunications. La téléphonie classique, qui a pour objet de transmettre la parole, a été gagnée de vitesse par l'échange de vastes quantités de données, qui peuvent être vocales, documentaires, musicales, photographiques et filmiques. Cet échange ne se déroule plus uniquement entre les êtres humains, mais intervient également entre êtres humains et ordinateurs et entre ordinateurs. Les connexions en mode circuit ont cédé la place à des réseaux à commutation par paquets. La question ne se pose plus de savoir si l'on peut établir une connexion directe : il suffit que les données soient saisies dans un réseau avec une adresse de destination ou mises à la disposition de tous ceux qui souhaitent y accéder.

3. La généralisation de l'utilisation du courrier électronique et de l'accès à une foule de sites web par l'Internet sont des exemples de cette évolution qui ont révolutionné notre société.

4. La facilité avec laquelle on peut avoir accès à l'information contenue dans les systèmes informatiques et la consulter a, couplée aux possibilités pratiquement illimitées d'échange et de diffusion de cette information, par delà les distances géographiques, déclenché une explosion de l'information disponible et des connaissances que l'on peut en tirer.

5. Ces développements ont donné lieu à des changements économiques et sociaux sans précédent, mais ils n'ont pas que des bons côtés : ils ont également fait apparaître de nouveaux types de délinquance et suscité la commission de délits classiques à l'aide des nouvelles technologies. Qui plus est, la délinquance peut avoir des conséquences de plus lourde portée que par le passé dans la mesure où elle ne se cantonne plus à un espace géographique donné et ne se soucie guère des frontières nationales. La propagation récente à travers le monde de virus informatiques dommageables témoigne bien de cette nouvelle réalité. Il importe de mettre en place des mesures techniques de protection des systèmes informatiques en même temps que des mesures juridiques de prévention et de dissuasion de la délinquance.

6. Les nouvelles technologies bousculent les principes juridiques existants. L'information et la communication circulent plus facilement que jamais à travers le monde. Les frontières ne peuvent plus s'y opposer. De plus en plus souvent les délinquants se trouvent dans des lieux fort éloignés de ceux où leurs actes produisent leurs effets. Or, les lois internes ne sont généralement applicables qu'à un territoire donné. Aussi les solutions aux problèmes posés relèvent-elles du droit international, ce qui nécessite l'adoption d'instruments juridiques internationaux adéquats. La présente Convention se propose de relever le défi ainsi posé, en tenant dûment compte de la nécessité de respecter les droits de l'homme dans la nouvelle société de l'information.

II. Les travaux préparatoires

7. Par sa décision CDPC/103/211196, le Comité européen pour les problèmes criminels (CDPC) a décidé en novembre 1996 de créer un comité d'experts chargés de la cybercriminalité. Le CDPC a motivé sa décision comme suit :

8. « Les rapides progrès des techniques de l'information ont des répercussions directes sur tous les secteurs de la société moderne. L'intégration des systèmes de télécommunication et d'information, en permettant le stockage et la transmission – quelle que soit la distance – de toutes sortes de données, ouvre un immense champ de possibilités nouvelles. Ces progrès ont été favorisés par l'apparition des réseaux informatiques et des autoroutes de l'information, notamment l'Internet, grâce auxquels toute personne ou presque peut avoir accès à la totalité des services d'information électronique, où qu'elle se trouve sur la planète. En se connectant aux services de communication et d'information, les usagers créent une sorte d'espace commun, dit "cyber-espace", qui sert à des fins légitimes, mais peut aussi donner lieu

à des abus. Les infractions commises dans ce cyber-espace le sont contre l'intégrité, la disponibilité et la confidentialité des systèmes informatiques et des réseaux de télécommunication, à moins qu'elles ne consistent en l'utilisation de ces réseaux ou de leurs services dans le but de commettre des infractions classiques. Le caractère international des infractions en question – par exemple celles commises au moyen de l'Internet – se heurte à la territorialité des institutions nationales de répression.

9. Le droit pénal doit donc suivre le rythme de ces évolutions techniques, qui offrent des moyens extrêmement perfectionnés d'employer à mauvais escient les services du cyber-espace et de porter ainsi atteinte à des intérêts légitimes. Etant donné que les réseaux informatiques ignorent les frontières, un effort international concerté s'impose pour faire face à de tels abus. La Recommandation n° R (89) 9 a certes permis de rapprocher les conceptions nationales touchant certaines formes d'emploi abusif de l'ordinateur, mais seul un instrument international contraignant pourrait avoir l'efficacité nécessaire dans la lutte contre ces nouveaux phénomènes. Un tel instrument devrait non seulement prévoir des mesures de coopération internationale, mais aussi traiter de questions de droit matériel et procédural, ainsi que de facteurs liés à l'emploi des techniques informatiques.»

10. En outre, le CDPC a tenu compte du rapport établi – à sa demande – par le Professeur H.W.K. Kaspersen, qui concluait en ces termes : « ... il faudrait s'en remettre à un autre instrument juridique qui engage davantage qu'une Recommandation, comme une Convention. Cette Convention devrait traiter non seulement de questions de droit pénal matériel, mais aussi de problèmes de procédure pénale ainsi que des procédures et instruments internationaux en matière de droit pénal. »¹ Une conclusion analogue figure dans le Rapport annexé à la Recommandation n° R (89) 9² concernant le droit matériel et dans la Recommandation n° R (95) 13³ relative aux problèmes de procédure pénale liés aux technologies de l'information.

11. Le mandat spécifique du nouveau comité était le suivant :

-
1. Application de la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur, Rapport établi par le Professeur H.W.K. Kaspersen (document CDPC (97) 5 et PC-CY (97) 5, page 106).
 2. Voir La Criminalité liée à l'ordinateur, Rapport du Comité européen pour les problèmes criminels, page 86.
 3. Voir Problèmes de procédure pénale liés à la technologie de l'information, Recommandation n° R (95) 13, principe n° 17.

- i. « Examiner, à la lumière de la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur et de la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information, en particulier les questions ci-après :
- ii. les infractions commises dans le cyber-espace, en particulier celles dont les auteurs se servent des réseaux de communication, l'Internet notamment : par exemple, transactions financières illicites, offre de services tombant sous le coup de la loi, violation des droits d'auteur et agissements contraires à la dignité humaine et à la législation sur la protection des mineurs ;
- iii. les autres questions de droit pénal matériel qui peuvent nécessiter une approche commune en vue d'une coopération internationale, comme les définitions, les sanctions et la responsabilité des parties concernées, y compris les personnes qui offrent des services sur l'Internet ;
- iv. le recours à des pouvoirs coercitifs – y compris la possibilité d'y recourir sur le plan international –, ainsi que la viabilité de tels recours dans un environnement technique ; ces derniers peuvent consister, par exemple, en l'interception de télécommunications et en la surveillance électronique des réseaux d'information (via l'Internet, entre autres), en des recherches et saisies dans les systèmes de traitement des données, y compris les sites Internet, en une action consistant à rendre inaccessible le matériel illicite et à imposer aux personnes qui offrent des services le respect d'obligations spéciales, compte tenu des problèmes posés par certaines mesures destinées à assurer la sécurité de l'information (par exemple le chiffrement) ;
- v. la question de la compétence vis-à-vis des infractions informatiques, par exemple la détermination du lieu (*locus delicti*) où l'infraction a été commise et du droit applicable en l'espèce, y compris le problème du *ne bis idem* en cas de multiplicité de compétences et le mode de résolution des conflits positifs de compétences et de prévention des conflits négatifs de compétences ;
- vi. les questions de coopération internationale dans les enquêtes sur les infractions ayant pour cadre le cyber-espace, en étroite coopération avec le Comité d'experts sur le fonctionnement des conventions européennes dans le domaine pénal (PC-OC).

Le Comité devra rédiger un instrument juridique contraignant fondé, autant que possible, sur les points i) à v) ci-dessus, en insistant particulièrement sur

les questions internationales et, au besoin, des recommandations annexes sur certains points. Il pourra formuler des suggestions concernant d'autres questions à examiner en tenant compte de l'évolution technique.»

12. Comme suite à la décision du CDPC, le Comité des Ministres a créé le nouveau comité, appelé « Comité d'experts sur la criminalité dans le cyber-espace (PC-CY) », par sa décision n° CM/Del/Dec(97)583, prise à la 583^e réunion des délégués des Ministres (tenue le 4 février 1997). Le PC-CY a commencé ses travaux en avril 1997 et s'est attelé à la négociation d'un projet de convention internationale sur la cybercriminalité. En vertu de son mandat initial, le Comité devait avoir achevé ses travaux le 31 décembre 1999. Comme, à cette date, il n'avait pas encore pu achever la négociation de certaines questions soulevées par le projet de Convention, son mandat a été prorogé jusqu'au 31 décembre 2000 par la décision n° CM/Del/Dec(99)679 des délégués des Ministres. Les Ministres européens de la justice ont à deux reprises exprimé leur appui à la négociation : par la Résolution n°1, adoptée à leur 21^e Conférence (Prague, juin 1997), dans laquelle ils recommandaient au Comité des Ministres d'appuyer les travaux entrepris par le CDPC sur la cybercriminalité en vue de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens efficaces d'enquête sur les infractions de ce type, et par la Résolution n° 3, adoptée à la 23^e Conférence des Ministres européens de la justice (Londres, juin 2000), dans laquelle ces derniers encourageaient les parties à la négociation à continuer de rechercher des solutions appropriées visant à permettre au plus grand nombre d'Etats possible de devenir parties à la Convention et considéraient qu'il importait de mettre en place un système rapide et efficace de coopération internationale qui tiendrait dûment compte des exigences spécifiques de lutte contre la cybercriminalité. Les Etats membres de l'Union européenne ont déclaré, dans une position commune adoptée en mai 1999, qu'ils appuyaient les travaux du PC-CY.

13. Entre avril 1997 et décembre 2000, le PC-CY a tenu 10 séances plénières et 15 séances de son Groupe de rédaction à participation non limitée. A la suite de l'expiration de la prorogation de son mandat, les experts ont tenu, sous les auspices du CDPC, trois séances supplémentaires pour mettre au point le projet de rapport explicatif et examiner le projet de Convention à la lumière de l'avis de l'Assemblée parlementaire. Le Comité des Ministres a prié l'Assemblée, en octobre 2000, de donner un avis sur le projet de Convention, qu'elle a adopté lors de la 2^e partie de sa session plénière d'avril 2001.

14. En vertu d'une décision prise par le PC-CY, une version provisoire du projet de convention a été déclassifiée et publiée en avril 2000 ; les versions suivantes ont aussi été rendues publiques, après chaque réunion plénière, pour permettre aux Etats négociateurs de consulter toutes les parties intéressées. Ce processus de consultation s'est avéré utile.

15. La version révisée et définitive du projet de Convention et du rapport explicatif y afférent a été présentée pour approbation au CDPC à sa 50^e session en juin 2001, à la suite de quoi le texte du projet de Convention a été présenté au Comité des Ministres pour adoption et ouverture à la signature.

III. La Convention

16. La Convention vise pour l'essentiel 1) à harmoniser les éléments des infractions ayant trait au droit pénal matériel national et les dispositions connexes en matière de cybercriminalité, 2) à fournir au droit pénal procédural national les pouvoirs nécessaires à l'instruction et à la poursuite d'infractions de ce type ainsi que d'autres infractions commises au moyen d'un système informatique ou dans le cadre desquelles des preuves existent sous forme électronique, et 3) à mettre en place un régime rapide et efficace de coopération internationale.

17. La Convention comprend donc quatre chapitres : I) Emploi des termes ; II) Mesures à prendre au niveau national – droit matériel et droit procédural ; III) Coopération internationale ; IV) Clauses finales.

18. La Section 1 du chapitre II (questions de droit matériel) porte sur les dispositions relatives aux incriminations et les autres dispositions connexes applicables à la criminalité informatique : il commence par définir 9 infractions groupées en quatre catégories, puis traite des autres formes de responsabilité et de sanctions. La Convention définit les infractions ci-après : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs, falsification informatique, fraude informatique, infractions se rapportant à la pornographie enfantine et infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

19. La Section 2 du chapitre II (questions de droit procédural) – dont la portée dépasse les infractions définies à la Section 1 en ce qu'elle s'applique à toute infraction commise au moyen d'un système informatique ou dans le cadre de laquelle des preuves existent sous forme électronique – commence par fixer les conditions et sauvegardes communes applicables à tous les pouvoirs

de procédure visés dans ce chapitre. Il énonce ensuite les pouvoirs de procédure suivants : conservation rapide de données stockées dans un système informatique ; conservation et divulgation rapides de données relatives au trafic ; injonction de produire ; perquisition et saisie de données informatiques stockées ; collecte en temps réel des données relatives au trafic ; interception de données relatives au contenu. Le chapitre II s'achève sur des dispositions relatives à la compétence.

20. Le chapitre III contient les dispositions relatives à l'entraide dans le domaine de la criminalité classique et informatique ainsi qu'aux règles d'extradition. Il traite de l'entraide classique dans deux situations : celle où aucun fondement juridique (traité, législation réciproque, etc.) n'existe entre les parties – auquel cas les dispositions de ce chapitre s'appliquent – et celle où un fondement juridique existe – auquel cas les modalités existantes s'appliquent également à l'entraide prévue par la présente Convention. L'entraide se rapportant à la criminalité informatique s'applique aux deux situations et s'étend, sans préjudice de conditions supplémentaires, à la même gamme de pouvoirs procéduraux que celle définie au chapitre II. En outre, le chapitre III contient une disposition relative à un type spécifique d'accès transfrontière à des données stockées qui ne nécessite pas l'entraide (« avec consentement ou lorsqu'elles sont accessibles au public ») et prévoit la mise en place d'un réseau 24/7 d'entraide rapide entre les Parties.

21. Enfin, le chapitre IV contient les clauses finales qui – à quelques exceptions près – reprennent les dispositions types des traités du Conseil de l'Europe.

Commentaire sur les articles de la Convention

Chapitre 1 – Terminologie

Introduction concernant les définitions de l'article 1

22. Les rédacteurs estiment qu'en vertu de la convention, les Parties ne seront pas tenues de reproduire mot pour mot, dans leurs lois internes, les quatre notions définies à l'article 1, à condition que ces lois couvrent ces notions d'une façon qui soit compatible avec les principes de la Convention et offrent un cadre équivalent pour sa mise en œuvre.

Article 1 (a) – Système informatique

23. Aux fins de la Convention, un système informatique est un dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé

des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau. « Automatisé » signifie sans intervention humaine directe, le « traitement des données » est un ensemble d'opérations appliquées à des données et effectuées par le biais de l'exécution d'un programme informatique. Un « programme informatique » est un ensemble d'instructions pouvant être exécutées par l'ordinateur pour obtenir le résultat attendu. Un ordinateur peut exécuter différents programmes. Dans un système informatique, on distingue généralement plusieurs composantes, à savoir le processeur ou l'unité centrale, et les périphériques. Par « périphérique », on entend un dispositif qui remplit certaines fonctions spécifiques en interaction avec l'unité centrale : imprimante, écran, lecteur/graveur de CD-ROM ou autre moyen de stockage, par exemple.

24. Un réseau est une interconnexion entre deux systèmes informatiques ou plus. Les connexions peuvent être reliées à la terre (fil ou câble, par exemple), sans fil (radio, infrarouge ou satellite, par exemple), ou les deux. Un réseau peut être géographiquement limité à une zone peu étendue (réseau local) ou couvrir une zone étendue (réseau étendu), et de tels réseaux peuvent eux-mêmes être interconnectés. L'Internet est un réseau mondial composé de nombreux réseaux interconnectés, qui utilisent tous les mêmes protocoles. Il existe encore d'autres types de réseaux, connectés ou non à l'Internet, capables de faire circuler des données entre des systèmes informatiques. Les systèmes informatiques peuvent être connectés au réseau en tant que points de sortie ou comme moyen de faciliter la transmission de l'information (routeurs et dispositifs similaires, par exemple). L'important, c'est que les données soient échangées sur le réseau.

Article 1 (b) – Données informatiques

25. La définition des données informatiques repose sur la définition des données établie par l'ISO. Cette définition comporte les mots « qui se prête à un traitement ». Cela signifie que les données sont mises sous une forme qui permet leur traitement direct par le système informatique. Pour indiquer clairement qu'aux fins de la Convention, il faut entendre par « données » des données sous forme électronique, ou sous une autre forme qui permet de les traiter directement, on a introduit la notion de « données informatiques ». Des données informatiques traitées de façon automatisée peuvent être la cible de l'une des infractions pénales définies

dans la Convention ou faire l'objet de l'une des mesures d'investigation définies par la Convention.

Article 1 (c) – Fournisseur de service

26. L'expression « fournisseur de service » englobe de nombreuses catégories de personnes jouant un rôle particulier dans la communication ou le traitement de données sur des systèmes informatiques (voir aussi les commentaires sur la section 2). Au point (i) de la définition, il est précisé que l'expression désigne notamment les entités publiques et privées qui offrent aux utilisateurs la possibilité de communiquer entre eux. Il est donc indifférent que les utilisateurs forment un groupe fermé ou que le fournisseur offre ou non ses services au public, gratuitement ou contre le paiement de droits. Le groupe fermé peut être constitué par les salariés d'une entreprise privée auxquels les services sont fournis par un réseau d'entreprise.

27. Au point (ii) de la définition, il est signalé que l'expression « fournisseur de services » s'applique aussi aux entités qui stockent des données, ou les traitent d'une autre façon, pour le compte des personnes mentionnées au point (i). En outre, l'expression englobe les entités qui stockent ou traitent des données pour les utilisateurs des services proposés par les personnes visées au point (i). Ainsi, en application de cette définition, les « fournisseurs de services » peuvent être des personnes qui proposent un service d'hébergement ou de mise en antémémoire (« cache »), ou une connexion à un réseau. Toutefois, la définition n'est pas destinée à s'appliquer à un simple fournisseur de contenu (à une personne qui passe un contrat avec un fournisseur d'hébergement pour qu'il héberge son site Web, par exemple), si celui-ci ne propose pas en outre des services de communication ou d'autres services de traitement des données.

Article 1 (d) – Données relatives au trafic

28. Aux fins de la Convention, les données relatives au trafic, telles qu'elles sont définies à l'article 1, alinéa d., constituent une catégorie de données informatiques soumises à un régime juridique particulier. Ces données sont produites par des ordinateurs appartenant à la chaîne de communication pour acheminer une communication de son origine à sa destination. Elles sont donc des auxiliaires de la communication elle-même.

29. Lors d'une enquête sur une infraction pénale concernant un système informatique, les données relatives au trafic sont nécessaires pour trouver la

source de la communication ; c'est un point de départ permettant de réunir d'autres preuves ou un élément constitutif de la preuve de l'infraction. Les données relatives au trafic pouvant être éphémères, il importe de faire en sorte qu'elles soient préservées dans des délais très brefs. Par conséquent, il peut être nécessaire de les divulguer rapidement pour connaître l'itinéraire de la communication et réunir d'autres preuves avant qu'elles ne soient effacées ou pour identifier un suspect. La procédure ordinaire de collecte et de divulgation de données informatiques risque donc d'être insuffisante. Par ailleurs, on considère en principe que la collecte de données relatives au trafic est une intrusion moins importante, car elle ne révèle pas le contenu de la communication, jugé plus sensible.

30. La définition dresse la liste exhaustive des catégories de données relatives au trafic qui sont soumises à un régime particulier dans la Convention : origine de la communication, destination, itinéraire, heure (GMT), date, taille, durée et type du service sous-jacent. Ces catégories ne seront pas toujours toutes techniquement accessibles, susceptibles d'être produites par un fournisseur de service, ni nécessaires à l'enquête pénale. Par « origine », on entend un numéro de téléphone, une adresse IP ou un moyen similaire d'identifier un dispositif de communication auquel un prestataire de services fournit des. La « destination » désigne une indication comparable concernant un dispositif de communication vers lequel des communications sont transmises. L'expression « type du service sous-jacent » renvoie au type du service utilisé au sein du réseau : transfert de fichiers, courrier électronique ou messagerie instantanée.

31. La définition laisse aux législateurs nationaux la capacité d'introduire des différenciations dans la protection juridique des données relatives au trafic, en fonction de leur sensibilité. Dans ce contexte, l'article 15 impose aux Parties de prévoir les conditions et sauvegardes adéquates, eu égard à la protection des droits de l'homme et des libertés fondamentales. Cela implique, entre autres, que les critères de fond et la procédure concernant l'exercice des pouvoirs d'investigation puissent varier en fonction de la sensibilité des données.

Chapitre II – Mesures à prendre au niveau national

32. Le chapitre II (articles 2 à 22) contient trois sections : droit pénal matériel (articles 2 à 13), droit de procédure (articles 14 à 21) et compétence (article 22).

Section 1 – Droit pénal matériel

33. La section 1 de la Convention (articles 2 à 13) a pour objet d'améliorer les moyens de prévenir et de réprimer la criminalité informatique en fixant une norme minimale commune permettant d'ériger certains actes en infractions pénales. Une harmonisation de ce type facilite la lutte contre cette criminalité aux niveaux national et international. La concordance entre les législations internes peut s'opposer à ce que des actes illicites soient commis de préférence dans une Partie qui appliquait antérieurement une norme moins stricte. De la sorte, il devient également possible de stimuler l'échange de données d'expérience communes utiles. La coopération internationale (en particulier l'extradition et l'entraide judiciaire) est facilitée, par exemple en ce qui concerne la règle de la double incrimination.

34. La liste des infractions présentée dans cette section représente un consensus minimal qui n'exclut pas qu'elle soit complétée en droit interne. Elle se fonde largement sur les principes directeurs élaborés en liaison avec la Recommandation n° R (89) 9 du Conseil de l'Europe sur la criminalité en relation avec l'ordinateur, et sur les travaux d'autres organisations internationales publiques et privées (OCDE, ONU, AIDP), mais tient également compte de pratiques illicites plus récentes liées à l'expansion des réseaux de télécommunications.

35. La section est divisée en cinq titres. Le titre 1 englobe les infractions informatiques les plus essentielles, à savoir les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques, qui représentent les principales menaces qui, d'après le débat conduit sur la sécurité des ordinateurs et des données, pèsent sur les systèmes de traitement et de transmission automatisés des données. Ce titre décrit le type d'infractions relevant de cette rubrique, à savoir l'accès non autorisé et l'altération illicite de systèmes, programmes ou données. Les titres 2 à 4 traitent d'autres types d'« infractions informatiques », qui jouent un plus grand rôle dans la pratique et qui consistent à utiliser les systèmes informatiques et de télécommunications pour attaquer certains intérêts juridiques qui, en règle générale, sont déjà protégés par le droit pénal contre les attaques menées à l'aide de moyens classiques. Les infractions regroupées dans le titre 2 (fraude et falsification informatiques) ont été ajoutées comme suite aux suggestions faites dans le cadre des principes directeurs élaborés en liaison avec la Recommandation n° R (89) 9 du Conseil de l'Europe. Le titre 3 porte sur les infractions se rapportant au contenu à savoir la production ou la diffusion illicites de pornographie enfantine par le biais de systèmes informatiques, qui représente l'un des

modes d'exécution d'une infraction les plus dangereux qui aient récemment fait leur apparition. Le comité de rédaction a examiné la possibilité d'inclure d'autres infractions se rapportant au contenu, telles que la diffusion de propagande raciste par le biais de systèmes informatiques. Cependant, le comité n'a pas été en mesure de parvenir à un consensus sur la criminalisation d'un tel comportement. L'idée d'inclure cette diffusion en tant qu'infraction pénale a été largement appuyée, mais certaines délégations ont émis de sérieuses réserves, en invoquant la liberté d'expression. Compte tenu de la complexité de la question, il a été décidé que le comité soumettrait au Comité européen pour les problèmes criminels (CDPC) la suggestion d'élaborer un Protocole additionnel à la présente Convention.

Le titre 4 énonce les « infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes ». Celles-ci figurent dans la Convention car les atteintes à la propriété intellectuelle sont l'une des formes de criminalité informatique les plus répandues et prenant des proportions jugées préoccupantes dans le monde entier. Enfin, le titre 5 englobe des dispositions supplémentaires sur la tentative et complicité et sur les sanctions et les mesures, et, conformément aux instruments internationaux récents, sur la responsabilité des personnes morales.

36. Les dispositions de droit matériel s'appliquent à des infractions commises au moyen des technologies de l'information, mais la Convention utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures.

37. Les auteurs de la Convention ont présumé que les Parties peuvent exclure les infractions mineures ou insignifiantes du champ d'application des articles 2 à 10.

38. Les infractions énumérées ont un trait particulier, à savoir que leurs auteurs doivent expressément agir « sans droit ». Cette expression rend compte du fait que le comportement décrit n'est pas toujours punissable en soi, mais peut être légal ou justifié non seulement par des exceptions légales classiques (consentement, légitime défense ou nécessité), mais dans les cas où d'autres principes ou intérêts excluent toute responsabilité pénale. L'expression « sans droit » tire son sens du contexte dans lequel elle est utilisée. Ainsi, sans restreindre la marge de manœuvre qu'ont les Parties pour interpréter ce concept dans leur droit interne, cette expression peut renvoyer à un comportement qui ne repose sur aucune compétence (législative, exécutive, administrative,

judiciaire, contractuelle ou consensuelle) ou à un comportement qui n'est couvert ni par des exceptions légales, excuses et faits justificatifs établis, ni par des principes de droit interne pertinents. La Convention ne concerne pas, par conséquent, les comportements conformes aux compétences gouvernementales légales (par exemple, lorsque le gouvernement de la Partie concernée agit dans un but de maintien de l'ordre public, de protection de la sécurité nationale ou dans le cadre d'une instruction pénale). De plus, les activités légitimes et ordinaires inhérentes à la conception des réseaux ainsi que les pratiques d'exploitation ou de commerce légitimes et ordinaires ne devraient pas être érigées en infractions pénales. On trouvera dans la partie correspondante du texte du rapport explicatif ci-après des exemples précis de telles exceptions au principe de l'incrimination. Il appartient aux Parties de déterminer les modalités d'application desdites exceptions dans leur ordre juridique interne (en droit pénal ou autre).

39. Toutes les infractions énumérées dans la Convention doivent être commises de façon « intentionnelle » pour que la responsabilité pénale soit engagée. Dans certains cas, un élément intentionnel spécifique supplémentaire fait partie intégrante de l'infraction. Ainsi, par exemple, à l'article 8 concernant la fraude informatique, l'intention d'obtenir un bénéfice économique est un élément constitutif de l'infraction. Les auteurs de la Convention se sont entendus pour considérer que l'interprétation du mot « intentionnellement » doit être laissée aux droits internes.

40. Certains articles de cette section permettent de subordonner l'application de la Convention en droit interne à des conditions restrictives. Dans d'autres cas, la Convention prévoit même l'éventualité de formuler une réserve (voir les articles 40 et 42). Ces différentes modalités d'application d'une approche plus restrictive de l'incrimination reflètent l'existence d'évaluations différentes de la dangerosité du comportement en question ou de la nécessité d'utiliser le droit pénal comme contre-mesure. Cette approche laisse aux gouvernements et aux parlements une marge de manœuvre pour arrêter leur politique pénale dans ce domaine.

41. Les lois instituant ces infractions devraient être rédigées de la façon la plus claire et spécifique possible de façon qu'il soit possible de prévoir le type de comportement qui entraînera une sanction pénale.

42. Au cours du processus de rédaction, les rédacteurs se sont demandé s'il était souhaitable d'incriminer aussi des comportements autres que ceux qui sont définis aux articles 2 à 11, notamment le « cybersquattage », c'est-à-dire

l'enregistrement d'un nom de domaine qui est identique soit au nom d'une entité existante et généralement connue, soit au nom commercial ou à la marque commerciale d'un produit ou d'une entreprise. Le « cybersquatteur » n'a aucune intention de faire un usage actif du nom de domaine ; il cherche à en retirer un avantage financier en forçant l'entité concernée, même indirectement, à racheter son nom de domaine pour en récupérer la propriété et le contrôle. Actuellement, on estime que ce comportement est lié à la question de la propriété industrielle et commerciale. Etant donné que la Convention ne porte pas sur les atteintes aux droits de propriété industrielle et commerciale, les rédacteurs n'ont pas jugé opportun de traiter de l'incrimination d'un tel comportement.

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

43. Les infractions pénales définies aux articles 2 à 6 ont pour but de protéger la confidentialité, l'intégrité et la disponibilité des systèmes ou données informatiques, non d'incriminer les activités légitimes et ordinaires inhérentes à la conception des réseaux ou bien les pratiques d'exploitation ou de commerce légitimes et ordinaires.

Accès illégal (article 2)

44. L'« accès illégal » vise l'infraction fondamentale consistant à créer une menace ou à attenter à la sécurité (c'est-à-dire la confidentialité, l'intégrité et la disponibilité) des systèmes et données informatiques. La nécessité d'une protection correspond à l'intérêt des organisations comme des particuliers de pouvoir diriger, exploiter et contrôler leurs systèmes sans perturbation et entrave d'aucune sorte. La simple intrusion non autorisée, à savoir le « piratage », le « craquage » ou l'« intrusion illicite dans un système informatique », devrait en principe être illégale en elle-même. Elle peut créer des obstacles pour les utilisateurs légitimes des systèmes et des données et peut entraîner l'altération ou la destruction et des coûts élevés de reconstruction. Ces intrusions peuvent donner accès à des données confidentielles (mots d'accès, informations sur le système cible) et à des secrets, permettre d'utiliser le système gratuitement, voire encourager les pirates à commettre des types plus dangereux d'infractions en relation avec l'ordinateur, telles que la fraude informatique ou la falsification informatique.

45. Le moyen le plus efficace de prévenir l'accès non autorisé est, naturellement, d'adopter et de mettre en place des mesures de sécurité efficaces.

Toutefois, la parade ne saurait être complète sans la menace et l'application de mesures de droit pénal. L'interdiction pénale de l'accès non autorisé permet d'accorder très tôt, au système et aux données en tant que tels, une protection supplémentaire contre les risques susvisés.

46. L'« accès » comprend la pénétration dans l'intégralité ou une partie quelconque d'un système informatique (matériel, composantes, données stockées du système installé, répertoires, données relatives au trafic et au contenu). Toutefois, il ne comprend pas le simple envoi de messages électroniques ou de fichiers au système en question. L'« accès » comprend la pénétration dans un autre système informatique accessible par les réseaux de télécommunications publics ou d'un système informatique connecté au même réseau, tel qu'un réseau local ou un intranet (réseau privé d'entreprise). Le mode de communication (par exemple à distance, y compris sans fil, ou rapprochée) n'entre pas en ligne de compte.

47. L'acte doit également être commis « sans droit ». En sus de l'explication de cette expression donnée plus haut, elle veut dire qu'il n'y a pas de pénalisation de l'accès autorisé par le propriétaire du système ou d'une partie de ce système ou par le détenteur d'un droit sur ce système (aux fins, par exemple, d'essai ou de protection autorisés du système informatique concerné). Il n'y a pas non plus d'incrimination de l'accès à un système informatique lorsque cet accès est libre et public, puisqu'on accède au système « avec droit ».

48. L'utilisation de certains outils techniques peut entraîner un accès au sens de l'article 2. C'est le cas de l'accès à une page Internet, directement ou en utilisant des liens hypertexte, y compris les deep-links, ou de l'application de « cookies » ou de « bots » pour situer et extraire des données. L'utilisation de ces outils n'est pas en soi « sans droit ». La gestion d'un site Web public implique que son propriétaire accepte que n'importe quel autre utilisateur du Web y ait accès. L'utilisation des outils standard prévus dans les protocoles et programmes de communication courants n'est pas en soi « sans droit », en particulier lorsque le détenteur du droit d'accès au système visé est réputé avoir accepté cette utilisation, comme dans le cas des « cookies » en s'abstenant de refuser la première livraison ou de l'éliminer.

49. La législation interne de nombreux pays contient déjà des dispositions concernant les infractions liées au « piratage », mais leur portée et leurs éléments constitutifs sont très variables. L'approche générale de la pénalisation qui se dégage de la première phrase de l'article 2 est controversée. Ceux qui y sont opposés font valoir que la simple intrusion ne crée pas nécessairement des

risques et qu'il arrive même que les actes de piratage permettent de détecter des failles ou des faiblesses dans la sécurité des systèmes. Ces considérations ont conduit certains pays à adopter une approche plus restrictive en exigeant des conditions supplémentaires pour que l'on puisse parler d'infraction, ce qui est également l'approche retenue par la Recommandation n° (89) 9 et celle proposée en 1985 par le Groupe de travail de l'OCDE.

50. Les Parties peuvent adopter l'approche générale et criminaliser le piratage pur et simple conformément à la première phrase de l'article 2. Selon une autre formule, elles peuvent fixer l'une ou la totalité des conditions énumérées dans la seconde phrase, en exigeant que l'infraction soit commise en violation des mesures de sécurité, dans l'intention spécifique d'obtenir des données informatiques ou dans une autre intention délictueuse engageant la responsabilité pénale, ou vis-à-vis d'un système informatique connecté à distance à un autre système informatique. Cette dernière option permet aux Parties d'exclure la situation dans laquelle une personne accède physiquement à un ordinateur autonome sans passer par un autre système informatique. Elles peuvent circonscrire l'infraction à l'accès illégal à des systèmes informatiques en réseaux (y compris les réseaux publics fournis par les services de télécommunications et les réseaux privés, tels que les intranets ou les extranets).

Interception illégale (article 3)

51. Cette disposition vise à protéger le droit au respect des données transmises. L'infraction représente la même violation du droit au respect des communications que l'écoute et l'enregistrement classiques des conversations téléphoniques entre des personnes. Le droit au respect de la correspondance est garanti par l'article 8 de la Convention européenne des droits de l'homme. L'infraction instituée par l'article 3 applique ce principe à toutes les formes de transfert électronique des données, que ce transfert s'effectue par téléphone, télécopieur, courrier électronique ou fichier.

52. Le texte de cette disposition reprend pour l'essentiel celui de l'infraction d'« interception non autorisée » figurant dans la Recommandation (89) 9. Dans la présente Convention, il a été précisé qu'il faut entendre par communications les « transmissions ... de données informatiques » ainsi que les émissions électromagnétiques dans les situations expliquées ci-après.

53. L'interception effectuée par des « moyens techniques » concerne l'écoute, le contrôle ou la surveillance du contenu des communications, et

l'obtention du contenu soit directement, au moyen de l'accès au système informatique et de son utilisation, soit indirectement, au moyen de l'emploi de dispositifs d'écoute. L'interception peut aussi consister en un enregistrement des données. Par moyens techniques, il faut entendre des dispositifs techniques connectés aux lignes de transmission ainsi que des dispositifs de collecte et d'enregistrement de communications sans fil. Ils peuvent consister en logiciels, mots d'accès et codes. L'exigence de l'utilisation de moyens techniques est une condition restrictive visant à éviter l'écueil de la surpénalisation.

54. L'infraction s'applique aux transmissions « non publiques » de données informatiques. Le terme « non publiques » qualifie la nature du moyen de transmission (communication), non la nature des données transmises. Il peut arriver que les données transmises soient disponibles pour tout le monde, mais que les participants souhaitent communiquer de façon confidentielle. Les données peuvent aussi être tenues secrètes à des fins commerciales jusqu'à ce que le service ait été rémunéré, comme pour la télévision payante. Il s'ensuit que le terme « non publiques » n'exclut pas en soi les communications par le biais des réseaux publics. Les communications de salariés, à des fins professionnelles ou non, qui constituent des « transmissions non publiques de données informatiques » sont aussi protégées contre l'interception sans droit en vertu de l'article 3 (voir, par exemple, l'arrêt rendu par la CEDH dans l'affaire *Halford c. Royaume-Uni*, 25 juin 1997, 20605/92).

55. La communication sous forme de transmission de données informatiques peut se dérouler à l'intérieur d'un même système informatique (c'est le cas de la circulation entre la carte unité centrale et l'écran ou l'imprimante), entre deux systèmes informatiques appartenant à la même personne, entre deux ordinateurs communiquant entre eux ou entre un ordinateur et une personne (par le biais du clavier, par exemple). Néanmoins, les Parties peuvent fixer comme condition supplémentaire que la communication soit transmise entre des systèmes informatiques connectés à distance.

56. Il convient de noter que la possibilité, pour le « système informatique », de couvrir aussi les liaisons radiophoniques ne signifie pas qu'une Partie soit tenue d'incriminer l'interception d'une transmission radio qui, bien que « non publique », se fait d'une manière relativement ouverte qui la rend aisément accessible, donc interceptable, notamment par des radio-amateurs.

57. L'institution d'une infraction relative aux émissions électromagnétiques élargira la portée de la disposition. Les émissions électromagnétiques peuvent

provenir d'un ordinateur en fonctionnement. Elles ne sont pas considérées comme des « données » au sens de la définition donnée à l'article 1. Cependant, des données peuvent être reconstituées à partir de telles émissions. Aussi a-t-on incorporé l'interception des données provenant d'émissions électromagnétiques produites par un système informatique parmi les infractions visées par la présente disposition.

58. Pour que la responsabilité pénale soit engagée, l'interception illégale doit être « intentionnelle » et « sans droit ». L'acte est justifié, par exemple, si la personne qui effectue l'interception est en droit de le faire, si elle agit sur ordre ou avec l'autorisation des participants à la transmission (y compris dans le cadre d'activités autorisées de contrôle ou de protection approuvées par les participants) ou si la surveillance est légalement autorisée par les autorités chargées d'une enquête dans l'intérêt de la sécurité nationale ou de la détection d'infractions. Il est également entendu que les pratiques commerciales ordinaires, telles que l'utilisation de « cookies », ne doivent pas être pénalisées en tant que telles, car il ne s'agit pas d'interception « sans droit ». S'agissant des communications non publiques de salariés protégées en vertu de l'article 3 (voir le paragraphe 54 ci-dessus), le droit interne peut prévoir un motif d'interception légitime de telles communications. Dans le cadre de l'article 3, une interception effectuée dans de telles conditions serait assimilée à une interception effectuée « avec droit ».

59. Dans certains pays, l'interception peut être étroitement liée à l'infraction d'accès non autorisé à un système informatique. Afin de garantir l'uniformité au niveau de l'interdiction et de l'application de la loi, les pays qui requièrent que l'infraction soit commise dans une intention délictueuse ou vis-à-vis d'un système informatique connecté à un autre système informatique, conformément à l'article 2, pourraient également requérir l'existence d'autres conditions à remplir pour que la responsabilité pénale soit engagée dans le cadre du présent article. Ces conditions devraient être interprétées et appliquées en combinaison avec d'autres éléments de l'infraction, tels que « intentionnellement » et « sans droit ».

Atteinte à l'intégrité des données (article 4)

60. Cette disposition vise à assurer aux données et programmes informatiques une protection analogue à celle dont jouissent les biens corporels à l'encontre des dommages occasionnés délibérément. En l'occurrence, les intérêts juridiques protégés sont l'intégrité et le bon fonctionnement ou le bon usage de données ou programmes informatiques enregistrés.

61. Au paragraphe 1, l'«endommagement» et la «détérioration», en tant qu'actes se chevauchant, concernent notamment l'altération négative de l'intégrité ou du contenu informatif de données et de programmes. L'effacement des données équivaut à la destruction d'objets corporels. Il les détruit et les rend méconnaissables. Par «suppression» des données informatiques, on entend tout acte à la suite duquel ces données ne sont pas ou plus accessibles à la personne ayant accès à l'ordinateur ou au support sur lequel les données étaient stockées. Le terme «altération» signifie la modification de données existantes. L'introduction de codes malveillants tels que des virus ou des chevaux de Troie relève donc des dispositions de ce paragraphe, de même que la modification des données qui résulte de cet acte.

62. Les actes susvisés ne sont punissables que s'ils sont commis «sans droit». Les activités ordinaires inhérentes à la conception des réseaux ou les pratiques ordinaires d'exploitation ou de commerce, comme, par exemple, celles qui correspondent aux essais ou à la protection de la sécurité d'un système informatique et sont autorisées par le propriétaire ou l'exploitant, ou à la reconfiguration du système d'exploitation d'un ordinateur qui se déroule lorsque l'exploitant d'un système acquiert un nouveau logiciel (c'est le cas des logiciels d'accès à l'Internet qui désactivent des programmes analogues installés antérieurement), sont légitimes et ne sont donc pas pénalisées par le présent article. En principe, la modification des données de trafic aux fins de faciliter les communications anonymes (comme dans le cas des activités des systèmes de réexpédition anonyme) ou la modification des données aux fins d'assurer la protection des communications (chiffrement, par exemple) sont considérées comme assurant la protection légitime de la vie privée et, de ce fait, sont considérées comme étant réalisées de façon légitime. Toutefois, les Parties peuvent incriminer certains actes abusifs se rapportant aux communications anonymes, comme dans le cas de la falsification des données d'un en-tête de paquet visant à dissimuler l'identité de l'auteur d'une infraction.

63. En outre, le délinquant doit avoir agi «intentionnellement».

64. Le paragraphe 2 autorise les Parties à faire une réserve concernant l'infraction, dans la mesure où elles peuvent exiger que le comportement doit entraîner un préjudice grave. Elles pourront interpréter l'expression «préjudice grave» comme elles le souhaitent dans leur droit interne, mais elles devront communiquer cette interprétation au Secrétaire Général du Conseil de l'Europe si elles utilisent cette possibilité de faire une réserve.

Atteinte à l'intégrité du système (article 5)

65. La Recommandation n° (89) 9 désigne cette rubrique sous l'appellation de sabotage informatique. Cette disposition vise à pénaliser l'entrave intentionnelle à l'usage légitime de systèmes informatiques, y compris de systèmes de télécommunications, en utilisant ou en influençant des données informatiques. Les intérêts juridiques à protéger sont l'intérêt des exploitants et des usagers d'un système informatique ou d'un système de télécommunications à ce que celui-ci soit en mesure de fonctionner correctement. Le texte est formulé de façon neutre de sorte qu'il puisse protéger toutes sortes de fonctions.

66. Le terme « entrave » se rapporte à des actions qui portent atteinte au bon fonctionnement du système informatique. L'entrave doit résulter de l'introduction, du transfert, de l'endommagement, de l'effacement, de l'altération ou de la suppression de données informatiques.

67. De plus, l'entrave doit être « grave » pour donner lieu à une sanction pénale. Il appartient à chaque Partie de déterminer les conditions à remplir pour que l'entrave puisse être considérée comme « grave. » Ainsi, par exemple, une Partie pourra exiger qu'un dommage d'une importance minimale ait été causé pour que l'on puisse parler d'entrave grave. Les auteurs ont jugé « grave » l'envoi à un système informatique de données dont la forme, le volume ou la fréquence porte un préjudice important à la capacité du propriétaire ou de l'exploitant d'utiliser le système en question ou de communiquer avec d'autres systèmes (c'est le cas des programmes qui portent atteinte à des systèmes sous la forme d'un « déni de service », des codes malveillants, tels que les virus, qui interdisent ou ralentissent sensiblement le fonctionnement du système, ou des programmes qui envoient un énorme volume de courrier électronique à un destinataire afin de paralyser les fonctions de communication du système).

68. L'entrave doit être « sans droit ». Les activités ordinaires inhérentes à la conception des réseaux ou les pratiques ordinaires d'exploitation ou de commerce sont commises « avec droit ». Il s'agit notamment des activités d'essai de la sécurité d'un système informatique ou de protection de ce système autorisées par son propriétaire ou exploitant, ou de la reconfiguration du système d'exploitation d'un ordinateur qui intervient lorsque l'exploitant d'un système installe un nouveau logiciel qui désactive des programmes analogues antérieurement installés. Ces activités ne sont donc pas incriminées par le présent article même si elles se traduisent par une entrave grave.

69. L'envoi, pour des motifs commerciaux ou autres, de messages électroniques à un destinataire qui n'a pas demandé à les recevoir risque de lui

causer des désagréments, notamment lorsque ces messages sont envoyés souvent ou en grandes quantités (« publipostage »). De l'avis des rédacteurs, un tel comportement ne devrait être criminalisé que dans le cas d'une entrave intentionnelle et grave à la communication. Toutefois, les Parties peuvent opter pour une conception différente de l'entrave dans leur droit interne, par exemple en faisant de certains actes d'ingérence des infractions administratives ou en les rendant passibles d'une sanction par un autre moyen. Le texte laisse aux Parties le soin de déterminer dans quelle mesure le fonctionnement du système doit être entravé – partiellement ou totalement, temporairement ou de façon permanente – pour que cette entrave justifie une sanction, administrative ou pénale, en vertu de leur droit interne.

70. L'infraction doit être commise intentionnellement ; en d'autres termes, son auteur doit avoir l'intention de causer une entrave grave.

Abus de dispositifs (article 6)

71. Cette disposition institue en infraction pénale distincte et indépendante la commission intentionnelle d'actes illicites spécifiques se rapportant à certains dispositifs ou données d'accès dont il est fait une utilisation abusive aux fins de commettre les infractions précitées contre la confidentialité, l'intégrité et la disponibilité des systèmes ou données informatiques. Dans la mesure où la commission desdites infractions nécessite souvent la possession de moyens d'accès (« outils de piratage ») ou d'autres outils, il existe une forte motivation d'en acquérir à des fins délictueuses, ce qui peut déboucher sur la création d'une sorte de marché noir de la production et de la distribution de tels outils. Pour parer plus efficacement ces risques, le droit pénal devrait interdire des actes spécifiques potentiellement dangereux à la source, avant la commission des infractions visées aux articles 2 à 5. A cet égard, la disposition s'appuie sur des instruments récemment adoptés par le Conseil de l'Europe (Convention européenne sur la protection juridique des services à accès conditionnel et des services d'accès conditionnel – STE n° 178) et l'Union européenne (Directive 98/84/EC du Parlement européen et du Conseil en date du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel), ainsi que sur les dispositions adoptées dans certains pays en la matière. Une approche analogue avait déjà été retenue dans la Convention de Genève de 1929 sur la contrefaçon de monnaie.

72. Le paragraphe 1.a)1) incrimine la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif, y compris un programme informatique, principalement conçu

pour permettre la commission de l'une des infractions établies aux articles 2 à 5 de la Convention. Par « diffusion », il faut entendre l'action consistant à transmettre des données à autrui, tandis que la « mise à disposition » désigne l'action consistant à mettre des dispositifs en ligne pour qu'ils soient utilisés par autrui. Cette expression englobe par ailleurs la création ou la compilation d'hyperliens visant à faciliter l'accès à ces dispositifs. La référence à un « programme informatique » concerne des programmes qui sont conçus, par exemple, pour altérer, voire détruire des données, ou pour s'ingérer dans le fonctionnement des systèmes, tels que les programmes-virus, ou bien des programmes conçus ou adaptés pour accéder à des systèmes informatiques.

73. Les auteurs ont longuement examiné la question de savoir si les dispositifs visés devaient être ceux qui étaient conçus exclusivement ou spécialement pour permettre la commission d'infractions, ce qui excluait les dispositifs à double usage. Cette approche a été jugée trop restrictive. Elle risquait en effet de créer des difficultés insurmontables en ce qui concerne l'établissement de la preuve dans les procédures pénales, ce qui rendrait la disposition pratiquement inapplicable ou applicable uniquement dans de rares cas. La solution consistant à inclure tous les dispositifs, même ceux dont la production et la diffusion sont licites, a également été écartée. L'imposition d'une sanction ne pourrait alors reposer que sur l'élément subjectif de l'intention de commettre une infraction informatique, approche qui n'avait pas non plus été retenue dans le domaine de la contrefaçon de monnaie. La Convention adopte une solution de compromis raisonnable en limitant le champ d'application de cette disposition aux dispositifs dont on peut objectivement dire qu'ils sont principalement conçus pour permettre la commission d'une infraction. Ce libellé exclut normalement les dispositifs à double usage.

74. Le paragraphe 1a)2) incrimine la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un mot de passe, d'un code d'accès ou des données informatiques similaires permettant d'accéder à l'ensemble ou à une partie d'un système informatique.

75. Le paragraphe 1b) érige en infraction pénale la possession des éléments visés aux paragraphes 1.a)1) ou 1.a)2). La dernière phrase du paragraphe 1.b) autorise les Parties à exiger en droit interne qu'un certain nombre de ces éléments soient détenus. Leur nombre sert directement à prouver l'intention délictueuse. Il appartient à chaque Partie d'arrêter le nombre d'éléments requis pour que la responsabilité soit engagée.

76. L'infraction doit être commise intentionnellement et sans droit. Avant d'éviter le risque de la surpénalisation lorsque des dispositifs sont fabriqués et commercialisés à des fins légitimes, par exemple pour contrer des atteintes aux systèmes informatiques, des critères supplémentaires sont ajoutés pour restreindre l'infraction. En sus de l'exigence générale de l'intention, il doit exister l'intention spécifique (c'est-à-dire directe) d'utiliser le dispositif pour commettre l'une ou l'autre des infractions visées aux articles 2 à 5 de la Convention.

77. Le paragraphe 2 énonce clairement que les outils créés pour l'essai autorisé ou la protection d'un système informatique ne relèvent pas du champ d'application de cette disposition. Cette notion est déjà exprimée dans la formule « sans droit ». Ainsi, par exemple, les dispositifs d'essai (« dispositifs de craquage ») et les dispositifs d'analyse de réseaux conçus par les milieux professionnels pour vérifier la fiabilité de leurs produits informatiques ou contrôler la sécurité des systèmes sont fabriqués à des fins légitimes et leurs utilisateurs sont donc considérés « avec droit ».

78. La nécessité d'appliquer l'infraction d'« abus de dispositifs » à toutes les catégories de délits informatiques visés aux articles 2 à 5 donnant lieu à des analyses différentes, le paragraphe 3 permet, au titre d'une réserve (voir article 42), de limiter l'infraction en droit interne. Toutefois, chaque Partie est tenue d'incriminer au moins la vente, la diffusion ou la mise à disposition d'un mot de passe ou des données d'accès visés au paragraphe 1.a)2).

Titre 2 – Infractions informatiques

79. Les articles 7 à 10 concernent des infractions ordinaires qui sont souvent commises au moyen d'un système informatique. La plupart des Etats ont déjà incriminé ces infractions ordinaires et la législation déjà en vigueur peut ou non être suffisamment souple pour inclure les cas d'utilisation de réseaux informatiques (par exemple, dans certains pays, les lois relatives à la pornographie enfantine peuvent ne pas s'appliquer aux images électroniques). Par conséquent, lors de la mise en œuvre de ces articles, les Etats doivent examiner leur droit interne pour déterminer s'il s'applique à des situations impliquant des systèmes ou des réseaux informatiques. Si les infractions existantes couvrent déjà ces comportements, il n'est nécessaire, ni de modifier ces incriminations, ni de définir de nouvelles infractions.

80. Les articles intitulés « Falsification informatique » et « Fraude informatique » se rapportent à certaines infractions informatiques, à savoir la falsification et la fraude informatiques en tant qu'il s'agit de deux types spécifiques de

manipulation des systèmes ou données informatiques. L'insertion de ces articles témoigne du fait que, dans bien des pays, certains intérêts juridiques traditionnels ne sont pas suffisamment protégés contre les nouvelles formes d'ingérence et d'attaques.

Falsification informatique (article 7)

81. Cet article a pour objet d'instituer une infraction qui soit le pendant de la falsification des documents sur papier. Elle vise à combler les lacunes du droit pénal se rapportant à la falsification classique, laquelle requiert la lisibilité visuelle des déclarations contenues dans un document et ne s'applique pas aux données enregistrées sur support électronique. La manipulation de données enregistrées ayant force probante peut avoir des conséquences aussi graves que les actes traditionnels de contrefaçon si elle induit un tiers en erreur. La falsification informatique consiste à créer ou modifier sans autorisation des données enregistrées de façon qu'elles acquièrent une valeur probante différente et que le déroulement de transactions juridiques, qui est fondé sur l'authenticité des informations fournies par ces données, puisse faire l'objet d'une tromperie. Les intérêts juridiques protégés sont la sécurité et la fiabilité des données électroniques qui peuvent avoir des conséquences pour les relations juridiques.

82. Il convient de noter que le concept de falsification varie beaucoup d'un pays à l'autre. Une notion est fondée sur l'authenticité quant à l'auteur du document, tandis que d'autres visent la véracité des informations contenues dans le document en question. Toutefois, il a été convenu que la tromperie quant à l'authenticité se rapporte au minimum à l'émetteur des données, indépendamment de l'exactitude ou de la véracité du contenu de ces données. Les Parties peuvent aller plus loin et prévoir que le terme « authentique » s'applique aussi aux données.

83. Cette disposition s'applique aux données équivalant à un document public ou privé ayant des effets juridiques. L'« introduction » non autorisée de données exactes ou inexactes crée une situation qui correspond à la fabrication d'un faux document. Les opérations ultérieures d'altération (modifications, changements partiels), d'effacement (le fait de sortir des données figurant sur un support) et de suppression (le fait de retenir et de cacher des données) correspondent en général à la falsification d'un document authentique.

84. L'expression « à des fins légales » s'applique également à des transactions et documents juridiques qui sont légalement pertinents.

85. La dernière phrase de la disposition permet aux Parties, au moment de mettre en œuvre l'infraction en droit interne, d'exiger en plus une intention frauduleuse ou une intention pernicieuse similaire pour que la responsabilité pénale puisse être engagée.

Fraude informatique (article 8)

86. La révolution technologique a multiplié les possibilités de commettre des infractions économiques telles que la fraude, notamment l'escroquerie aux cartes de crédit. Les actifs représentés ou gérés par des systèmes informatiques (fonds électroniques, dépôts) sont devenus la cible de manipulations au même titre que les formes traditionnelles de propriété. Ces infractions consistent pour l'essentiel en des manipulations à l'entrée du système, c'est-à-dire en introduisant dans l'ordinateur des données inexactes, en des manipulations de programmes ou en d'autres ingérences dans le traitement des données. Cet article a pour objet de rendre passible d'une sanction pénale toute manipulation abusive au cours d'un traitement de données en vue d'effectuer un transfert illicite de propriété.

87. Afin de veiller à ce que toutes les manipulations pertinentes possibles soient prises en compte, les éléments constitutifs que sont l'« introduction », l'« altération », l'« effacement » et la « suppression » visés à l'alinéa a) de l'article 8 sont complétés par l'acte général d'« atteinte au fonctionnement d'un système informatique » visé à l'alinéa b) de l'article 8. Les éléments que sont l'« introduction, l'altération, l'effacement ou la suppression » ont le même sens que dans les articles précédents. L'alinéa b de l'article 8 se rapporte à des actes tels que les manipulations de matériel, les actes empêchant les sorties sur imprimante et les actes affectant les enregistrements ou les flux de données, ou l'ordre dans lequel les programmes sont exécutés.

88. Les manipulations informatiques frauduleuses sont incriminées si elles occasionnent directement à autrui un préjudice économique ou matériel et si le délinquant a agi dans l'intention d'obtenir un avantage économique illégitime pour lui-même ou pour autrui. L'expression « préjudice économique ou matériel » correspond à une notion très large qui englobe l'argent et les immobilisations corporelles ou incorporelles ayant une valeur économique.

89. L'infraction doit être commise « sans droit », et l'avantage économique doit être obtenu sans droit. Naturellement, les pratiques commerciales ordinaires légitimes, effectuées dans l'intention de procurer un bénéfice économique, ne sauraient relever de l'infraction établie par cet article, car les personnes qui

s'y livrent sont dans leur droit. Par exemple, les activités menées en vertu d'un contrat en bonne et due forme passé entre les personnes concernées sont légitimes (comme celle consistant à désactiver un site Web, conformément aux termes du contrat en question).

90. L'infraction doit être commise « intentionnellement ». L'élément général d'intention s'applique à la manipulation ou à l'ingérence informatique causant un préjudice économique ou matériel à autrui. L'infraction exige également une intention frauduleuse spécifique ou autrement malhonnête en vue d'obtenir un avantage économique pour soi-même ou pour autrui. Ainsi, les activités commerciales relatives à la concurrence qui peuvent causer un préjudice économique à une personne et apporter un bénéfice à une autre, mais qui ne sont pas pratiquées dans une intention frauduleuse ou malhonnête, ne constituent pas une infraction au titre de l'article 8. Par exemple, l'utilisation de programmes de collecte d'informations pour faire jouer la concurrence sur l'Internet (« bots »), même si cette pratique n'est pas autorisée par un site visité par le « bot », ne devrait pas être incriminée.

Titre 3 – Infractions se rapportant au contenu

Infractions se rapportant à la pornographie enfantine (article 9)

91. L'article 9 relatif à la pornographie enfantine vise à renforcer les mesures de protection en faveur des enfants, notamment leur protection contre l'exploitation sexuelle, en modernisant le droit pénal de façon à restreindre plus efficacement l'usage des systèmes informatiques dans le cadre de la commission d'infractions sexuelles à l'encontre d'enfants.

92. Cette disposition répond à la préoccupation que les chefs d'Etat ou de gouvernement des pays membres du Conseil de l'Europe ont exprimée à leur 2^e sommet (Strasbourg, 10-11 octobre 1997) dans leur Plan d'action (point III.4) et correspond à une évolution internationale allant dans le sens de l'interdiction de la pornographie enfantine, comme l'attestent l'adoption récente du Protocole facultatif à la Convention des Nations Unies relative aux droits de l'enfant se rapportant à la vente d'enfants, à la prostitution des enfants et à la pornographie impliquant des enfants et la récente initiative de la Commission européenne sur la lutte contre l'exploitation sexuelle des enfants et la pornographie enfantine (COM2000/854).

93. Cette disposition incrimine différents aspects de la production, de la possession et de la diffusion de pornographie enfantine. La plupart des Etats

incriminent déjà la production traditionnelle et la diffusion physique de pédopornographie, mais étant donné que l'Internet est de plus en plus utilisé comme instrument principal pour l'échange de ce matériel, il a été considéré que des dispositions spécifiques dans un instrument juridique international pour lutter contre cette nouvelle forme d'exploitation sexuelle enfantine et de mise en danger des enfants étaient tout à fait essentielles. On s'accorde largement à reconnaître que ce matériel et les pratiques en ligne qui lui sont associées, telles que l'échange d'idées, de fantasmes et de conseils entre pédophiles, contribuent à appuyer, encourager ou faciliter les infractions sexuelles commises à l'encontre d'enfants.

94. Le paragraphe 1.a) érige en infraction pénale le fait de produire de la pornographie enfantine en vue de la diffuser par le biais d'un système informatique. Cette disposition a été jugée nécessaire pour combattre à la source les dangers susvisés.

95. Le paragraphe 1.b) érige en infraction pénale le fait d'« offrir » de la pornographie enfantine par le biais d'un système informatique. Le terme « offrir » vise à inclure le fait de solliciter autrui pour se procurer de la pornographie enfantine. Il laisse entendre que la personne qui offre le matériel en question peut effectivement le fournir. L'expression « rendre disponible » vise à inclure la mise en ligne de pornographie enfantine devant être utilisée par autrui, par exemple en créant des sites pédophiles. Ce paragraphe entend également s'appliquer à la création ou à la compilation d'hyperliens vers des sites pédophiles en vue de faciliter l'accès à la pornographie enfantine.

96. Le paragraphe 1.c) érige en infraction pénale le fait de diffuser ou de transmettre de la pornographie enfantine par le biais d'un système informatique. Par « diffusion », il faut entendre la distribution active du matériel incriminé. Le fait d'envoyer à autrui de la pornographie enfantine par le biais d'un système informatique relève de l'infraction consistant à « transmettre » de la pornographie enfantine.

97. Au paragraphe 1.d), l'expression « se procurer ou procurer à autrui » doit s'entendre du fait d'obtenir activement de la pornographie enfantine, par exemple par téléchargement.

98. Le paragraphe 1.e) érige en infraction pénale le fait de posséder de la pornographie enfantine dans un système informatique ou dans un moyen de stockage de données informatiques, comme une disquette ou un disque optique compact. Le fait de posséder de la pornographie enfantine stimule la demande de ce matériel. Un moyen efficace de mettre un frein à la production

de pornographie infantine consiste à rendre passible de sanctions pénales le comportement de chaque maillon de la chaîne allant de la production à la possession.

99. L'expression « matière pornographique » figurant au paragraphe 2 doit être interprétée conformément aux normes de droit interne concernant la classification du matériel comme obscène, incompatible avec les mœurs publiques ou ayant à un autre titre un effet pervers. Il s'ensuit que le matériel présentant un intérêt artistique, médical, scientifique, etc., pourra être considéré comme n'étant pas pornographique. Les moyens de représentation visuelle sont notamment les données stockées sur des disquettes informatiques ou d'autres moyens électroniques de stockage et pouvant être converties en images visuelles.

100. L'expression « comportement sexuellement explicite » désigne au moins l'un ou l'autre des comportements réels ou simulés suivants : a) relations sexuelles – y compris génito-génitales, oro-génitales, ano-génitales ou oro-anales – entre mineurs ou entre un mineur et un adulte, du même sexe ou de sexes opposés ; b) zoophilie ; c) masturbation ; d) violences sado-masochistes dans un contexte sexuel ; e) exhibition lascive des parties génitales ou de la région pubienne d'un mineur. Le fait que le comportement représenté soit réel ou simulé n'entre pas en ligne de compte.

101. Les trois types de matériel définis au paragraphe 2 aux fins de la commission des infractions visées au paragraphe 1 incluent les représentations d'un abus sexuel commis à l'encontre d'un enfant véritable [(2.a)], les images pornographiques représentant une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite [2.b)] et, enfin, les images qui, bien que « réalistes », ne représentent pas, en fait, un enfant véritable se livrant à un comportement sexuellement explicite [2.c)]. Dans ce dernier cas, il peut s'agir d'images altérées, telles que des images morphisées de personnes physiques, voire d'images totalement fabriquées par l'ordinateur.

102. Dans les trois cas visés au paragraphe 2, les intérêts juridiques protégés sont légèrement différents. Le paragraphe 2.a) concerne plus directement la protection des enfants contre la maltraitance. Les paragraphes 2. b) et 2.c) visent à offrir une protection contre un comportement qui, sans nécessairement causer un préjudice à l'« enfant » représenté dans le matériel en question, pourrait servir à encourager ou amener des enfants à participer à de tels actes et s'inscrit, de ce fait, dans le cadre d'une sous-culture préconisant la maltraitance des enfants.

103. L'expression « sans droit » n'exclut pas les exceptions et excuses légales, des faits justificatifs ou d'autres principes similaires qui exemptent une personne de la responsabilité pénale dans certaines circonstances particulières. Par conséquent, l'expression « sans droit » autorise une Partie à prendre en compte les droits fondamentaux tels que la liberté de pensée, la liberté d'expression et le droit au respect de la vie privée. En outre, une Partie peut prévoir une exception en ce qui concerne un comportement mettant en œuvre un « matériel pornographique » présentant un intérêt artistique, médical, scientifique ou autre intérêt similaire. S'agissant du paragraphe 2. b), l'expression « sans droit » pourrait également permettre à une Partie, par exemple, de prévoir qu'une personne est exempte de responsabilité pénale s'il est établi que l'individu représenté n'est pas « un mineur » au sens de cette disposition.

104. En ce qui concerne la pornographie infantine en général, le paragraphe 3 définit le terme « mineur » comme désignant toute personne âgée de moins de 18 ans, conformément à la définition d'un « enfant » donnée par la Convention des Nations Unies relative aux droits de l'enfant (article premier). On a considéré comme une importante question de principe l'établissement d'une norme d'âge internationale uniforme. Il convient de noter que l'âge se rapporte à l'utilisation d'enfants (réels ou fictifs) en tant qu'objets sexuels et est distinct de l'âge requis pour consentir à des relations sexuelles. Néanmoins, compte tenu du fait que certains Etats exigent une limite d'âge inférieure dans la législation nationale concernant la pornographie infantine, la dernière phrase du paragraphe 3 permet aux Parties d'exiger une limite d'âge différente, laquelle, en tout état de cause, ne doit pas être inférieure à 16 ans.

105. Cet article énumère différents types d'actes illicites se rapportant à la pornographie infantine que, comme dans les articles 2 à 8, les Parties sont tenues d'ériger en infractions pénales s'ils sont commis « intentionnellement. » En vertu de ce critère, une personne ne peut être responsable que si elle a l'intention d'offrir, de rendre disponible, de diffuser, de transmettre, de produire ou de posséder de la pornographie infantine. Les Parties peuvent adopter une norme plus spécifique (voir, par exemple, la législation de la Communauté européenne applicable à la responsabilité des fournisseurs de services), auquel cas c'est cette norme qui s'appliquerait. Ainsi, par exemple, la responsabilité peut être imposée s'il y a « connaissance et contrôle » de l'information transmise ou stockée. Il ne suffit pas, par exemple, qu'un fournisseur de services serve d'intermédiaire pour la transmission de ce

matériel, par le biais d'un site Web ou d'un bavardoir, entre autres moyens, en l'absence de l'intention requise en l'occurrence en droit interne. De plus, un fournisseur de services n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale.

106. Le paragraphe 4 permet aux Parties de formuler des réserves au sujet du paragraphe 1.d) et e) et du paragraphe 2.b) et c). Les Parties peuvent se réserver le droit de ne pas appliquer ces paragraphes en tout ou en partie. Toute réserve à ce sujet doit être déclarée au Secrétaire général du Conseil de l'Europe au moment de la signature ou du dépôt par la Partie concernée de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, conformément à l'article 42.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes (article 10)

107. Les atteintes aux droits de propriété intellectuelle, et en particulier au droit d'auteur, figurent parmi les infractions le plus communément commises sur l'Internet et préoccupent tant les détenteurs d'un droit d'auteur que les professionnels des réseaux informatiques. La reproduction et la diffusion sur l'Internet d'œuvres protégées sans l'autorisation du détenteur du droit d'auteur sont extrêmement fréquentes. Ces œuvres protégées sont notamment les œuvres littéraires, photographiques, musicales et audiovisuelles. La facilité avec laquelle des copies non autorisées peuvent être faites au moyen de la technologie numérique et l'échelle à laquelle elles sont reproduites et diffusées par le biais des réseaux électroniques ont imposé d'inclure des dispositions relatives aux sanctions pénales et de renforcer la coopération internationale dans ce domaine.

108. En vertu des instruments visés dans l'article, chaque Partie est tenue d'ériger en infraction pénale les atteintes délibérées à la propriété intellectuelle et aux droits connexes, parfois désignés sous le nom de droits voisins, lorsque ces atteintes ont été commises au moyen d'un système informatique et à une échelle commerciale ». Le paragraphe 1 prévoit des sanctions pénales contre les atteintes à la propriété intellectuelle commises au moyen d'un système informatique. L'atteinte au droit d'auteur est déjà une infraction dans presque tous les Etats. Le paragraphe 2 traite des atteintes aux droits connexes commises au moyen d'un système informatique.

109. Les atteintes à la propriété intellectuelle, comme les atteintes aux droits connexes, correspondent aux définitions qu'en donne la législation nationale de chaque Partie aux fins de l'exécution des obligations que celle-ci a souscrites en vertu de certains instruments internationaux. Chaque Partie est tenue d'ériger ces atteintes en infractions pénales, mais la définition précise de ces infractions en droit interne peut varier d'un Etat à l'autre. Toutefois, l'obligation d'incrimination découlant de la Convention ne couvre pas les atteintes à la propriété intellectuelle autres que celles qui sont mentionnées explicitement à l'article 10. Par conséquent, sont donc exclues les atteintes aux droits des brevets et des marques.

110. S'agissant du paragraphe 1, les instruments visés sont l'Acte de Paris du 24 juillet 1971, la Convention de Berne sur la protection des œuvres littéraires et artistiques, l'Accord sur les aspects commerciaux des droits de propriété intellectuelle (ADPIC) et le Traité de l'OMPI sur la propriété intellectuelle. En ce qui concerne le paragraphe 2, les instruments internationaux mentionnés sont la Convention internationale pour la protection des interprètes, exécutants, producteurs de phonogrammes et organisations de radiodiffusion (Convention de Rome), l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et le Traité de l'OMPI sur les interprétations, exécutions et phonogrammes. L'emploi du membre de phrase « conformément aux obligations que celle-ci a souscrites » dans les deux paragraphes spécifie qu'une Partie contractante à la présente Convention n'est pas tenue d'appliquer les instruments mentionnés auxquels elle n'est pas Partie ; de plus, si une Partie a fait une réserve ou une déclaration autorisée en vertu de l'un des instruments visés, cette réserve peut limiter l'étendue de l'obligation qui lui incombe en vertu de la présente Convention.

111. Au moment de la conclusion de la présente Convention, le Traité de l'OMPI sur la propriété intellectuelle et le Traité de l'OMPI sur les interprétations, exécutions et phonogrammes n'étaient pas entrés en vigueur. Ces traités n'en sont pas moins importants en ce qu'ils constituent une actualisation appréciable de la protection de la propriété intellectuelle (s'agissant en particulier du nouveau droit consistant à « rendre disponible » une œuvre protégée « à la demande » sur l'Internet) et qu'ils améliorent les moyens de lutter contre les violations des droits de propriété intellectuelle dans le monde entier. Toutefois, il a été considéré que les atteintes aux droits établies par lesdits Traités ne devront être érigées en infractions pénales en vertu de la présente Convention que lorsque ces traités seront entrés en vigueur en ce qui concerne une Partie.

112. L'obligation d'incriminer les atteintes à la propriété intellectuelle et aux droits connexes conformément aux obligations souscrites en vertu d'instruments internationaux ne s'étend à aucun droit moral conféré par les instruments mentionnés (tels que l'article 6bis de la Convention de Berne et l'article 5 du Traité de l'OMPI sur la propriété intellectuelle).

113. Les infractions se rapportant au droit d'auteur et aux droits connexes doivent avoir été commises « délibérément » pour que la responsabilité pénale soit engagée. A la différence de toutes les autres dispositions de droit matériel de cette Convention, le terme « délibérément » est utilisé au lieu de « intentionnellement » aux paragraphes 1 et 2 car c'est le terme employé dans l'accord ADPIC (article 61, concernant l'obligation d'ériger les violations du droit d'auteur en infractions pénales).

114. Les dispositions visent à imposer de sanctions pénales contre les atteintes commises « à une échelle commerciale » et au moyen d'un système informatique. Cela est conforme à l'article 61 de l'accord ADPIC, qui ne requiert de sanctions pénales en matière de violation du droit d'auteur que dans le cas de la « piraterie à une échelle commerciale ». Toutefois, les Parties peuvent souhaiter aller au-delà du seuil de l'« échelle commerciale » et incriminer également d'autres types d'atteinte à la propriété intellectuelle.

115. L'expression « sans droit » a été omise du texte de cet article car elle serait redondante : en effet, le terme « atteinte » dénote en lui-même l'utilisation sans autorisation d'une œuvre protégée par un droit d'auteur. L'absence de l'expression « sans droit » n'exclut pas *a contrario* les exceptions et excuses légales, des faits justificatifs ou d'autres principes similaires exemptant une personne de la responsabilité pénale qui sont associés à l'expression « sans droit » dans d'autres articles de la Convention.

116. Le paragraphe 3 permet aux Parties de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 dans des « circonstances bien délimitées » (par exemple les importations parallèles et les droits de location) dès lors que d'autres recours efficaces, notamment des mesures de caractère civil et/ou administratif, sont disponibles. Cette disposition constitue en substance pour les Parties une dérogation limitée à l'obligation d'imposer une responsabilité pénale, pour autant qu'elles ne dérogent pas aux obligations souscrites en vertu de l'article 61 de l'accord ADPIC, qui est la norme d'incrimination préexistante minimale.

117. Cet article ne doit en aucun cas être interprété comme étendant à des personnes qui ne satisfont pas aux critères définis par le droit interne ou

un accord international la protection accordée aux auteurs, réalisateurs de films, interprètes, exécutants, producteurs de phonogrammes, organismes de radiodiffusion ou autres détenteurs de droits.

Titre 5 – Autres formes de responsabilité et de sanctions

Tentative et complicité (article 11)

118. Cet article vise à établir des infractions supplémentaires se rapportant à la tentative de commettre les infractions définies par la Convention et la complicité en vue de leur perpétration. Comme on le verra plus loin, une Partie n'est pas tenue d'ériger en infraction pénale la tentative de commettre chaque infraction établie dans la Convention.

119. Aux termes du paragraphe 1, les Parties doivent ériger en infractions pénales tout acte de complicité en vue de la perpétration d'une des infractions établies en vertu des articles 2 à 10 de la Convention. La responsabilité est engagée en cas de complicité lorsque la personne qui commet une infraction établie par la Convention est aidée par une autre personne qui a également l'intention que l'infraction soit commise. Ainsi, par exemple, bien que la transmission par le biais de l'Internet de données relatives à un contenu nuisible ou d'un code malveillant requiert l'assistance de fournisseurs de services agissant comme intermédiaires, un fournisseur de services qui n'a pas d'intention criminelle ne peut être tenu responsable au titre de cette section. Les fournisseurs de services ne sont donc pas tenus de surveiller activement le contenu pour éviter la responsabilité pénale en vertu de cette disposition.

120. S'agissant du paragraphe 2 relatif à la tentative, on a jugé difficilement concevable que certaines infractions définies dans la Convention ou certains éléments desdites infractions puissent donner lieu à une tentative (c'est le cas, par exemple, des éléments relatifs au fait d'offrir ou de rendre disponible de la pornographie infantile). De plus, certains systèmes juridiques limitent les infractions pour lesquelles la tentative est sanctionnée. En conséquence, les Parties ne sont tenues d'incriminer la tentative que dans le cas des infractions établies en application des articles 3, 4, 5, 7, 8, 9.1)a) et 9.1)c).

121. Comme pour toutes les infractions établies en vertu de la Convention, la tentative et l'acte de complicité doivent être commis intentionnellement.

122. Le paragraphe 3 a été ajouté pour remédier aux difficultés que le paragraphe 2 pourrait causer aux Parties du fait de la grande variété d'approches retenues dans les législations nationales et malgré l'effort consenti

au paragraphe 2 pour éviter l'application à certains aspects de la disposition régissant la tentative. Une Partie peut déclarer qu'elle se réserve le droit de ne pas appliquer le paragraphe 2 en tout ou en partie. En d'autres termes, une partie faisant une réserve au sujet de cette disposition ne sera pas tenue d'incriminer la tentative quelles que soient les circonstances ou pourra choisir les infractions ou parties d'infractions pour lesquelles elle imposera des sanctions pénales au titre de la tentative. La réserve a pour but de permettre au plus grand nombre d'Etats possible de ratifier la Convention tout en permettant aux Parties de conserver certains de leurs principes juridiques fondamentaux.

Responsabilité des personnes morales (article 12)

123. L'article 12 traite de la responsabilité des personnes morales. Il est conforme à la tendance juridique actuelle à reconnaître la responsabilité des personnes morales. Il vise à imposer une responsabilité aux sociétés commerciales, associations et personnes morales similaires pour les actions criminelles commises pour leur compte par une personne exerçant un pouvoir de direction au sein de la personne morale. L'article 12 prévoit aussi une responsabilité lorsqu'une personne exerçant un pouvoir de direction omet de superviser ou de contrôler un employé ou un agent de la personne morale, dans les cas où une telle omission facilite la perpétration, par cet employé ou agent, de l'une des infractions définies dans la Convention.

124. En vertu du paragraphe 1, quatre conditions doivent être remplies pour que la responsabilité soit engagée. Premièrement, l'une des infractions définies dans la Convention doit avoir été commise. Deuxièmement, l'infraction doit avoir été commise pour le compte de la personne morale. Troisièmement, c'est une personne exerçant un pouvoir de direction qui doit l'avoir commise (y compris en tant que complice). L'expression « personne exerçant un pouvoir de direction » désigne une personne physique occupant un rang élevé dans l'organisation, comme le directeur. Quatrièmement, la personne exerçant un pouvoir de direction doit avoir agi sur la base de l'une de ses compétences – un pouvoir de représentation ou le pouvoir de prendre des décisions ou d'exercer un contrôle –, ce qui démontre que ladite personne physique a agi dans le cadre de son pouvoir d'engager la responsabilité de la personne morale. En résumé, le paragraphe 1 oblige les Parties à avoir la capacité d'imposer une responsabilité à la personne morale uniquement au titre des seules infractions commises par des personnes exerçant un pouvoir de direction.

125. En outre, le paragraphe 2 oblige les Parties à avoir la capacité d'imposer une responsabilité à une personne morale lorsque l'infraction est commise non

par la personne exerçant un pouvoir de direction visée au paragraphe 1, mais une autre personne agissant sous l'autorité de la personne morale, c'est-à-dire l'un de ses employés ou agents agissant dans le cadre de leur pouvoir. Les conditions à remplir pour que la responsabilité soit engagée sont les suivantes : 1) une infraction a été commise par un employé ou agent de la personne morale, 2) l'infraction a été commise pour le compte de la personne morale, et 3) la commission de l'infraction a été rendue possible par le fait que la personne exerçant un pouvoir de direction n'a pas supervisé l'employé ou l'agent en question. A cet égard, le défaut de supervision devrait être interprété comme incluant le fait de ne pas avoir pris des mesures appropriées et raisonnables pour empêcher les employés ou les agents de se livrer à des activités illégales pour le compte de la personne morale. La forme de ces mesures appropriées et raisonnables pourrait dépendre de plusieurs facteurs, tels que la nature de l'entreprise, sa taille, les normes applicables ou les bonnes pratiques en vigueur, etc. Il ne faudrait pas interpréter cette disposition comme imposant l'obligation d'établir un système général de surveillance des communications des employés (voir aussi le paragraphe 54). Un fournisseur de services ne peut être tenu responsable du fait qu'une infraction a été commise sur son système par un client, un usager ou un autre tiers, car l'expression « [personne physique] agissant sous son autorité » ne s'applique qu'aux employés et agents agissant dans le cadre de leur pouvoir.

126. La responsabilité visée par cet article peut être pénale, civile ou administrative. Il est loisible à chaque Partie de décider de prévoir l'une quelconque ou l'ensemble de ces formes de responsabilité, conformément à ses principes juridiques, dès l'instant que la forme de responsabilité retenue satisfait aux critères énoncés au paragraphe 2 de l'article 13, selon lesquels les sanctions ou mesures doivent être « effectives, proportionnées et dissuasives » et incluent les sanctions pécuniaires.

127. Le paragraphe 4 précise que la responsabilité des personnes morales n'exclut pas la responsabilité des personnes physiques.

Sanctions et mesures (article 13)

128. Cet article est étroitement lié aux articles 2 à 11, qui définissent différentes infractions informatiques ou en relation avec l'ordinateur qui doivent être rendues passibles de sanctions pénales. Conformément aux obligations imposées par ces articles, cette disposition oblige les Parties contractantes à tirer les conséquences de la gravité de ces infractions en prévoyant des sanctions pénales qui soient « effectives, proportionnées et dissuasives » et, dans

le cas des personnes physiques, incluent la possibilité d'imposer des peines d'emprisonnement.

129. Les personnes morales dont la responsabilité doit être établie en vertu de l'article 12 doivent également être exposées à des sanctions « effectives, proportionnées et dissuasives », pouvant être pénales, administratives ou civiles. Les Parties contractantes sont tenues, en application du paragraphe 2, de prévoir la possibilité d'imposer des sanctions pécuniaires aux personnes morales.

130. L'article laisse ouverte la possibilité d'imposer d'autres sanctions ou mesures adaptées à la gravité des infractions commises – par exemple des ordonnances d'interdiction ou de confiscation. Il laisse à l'appréciation des Parties la question de la création d'un système d'infractions et de sanctions pénales qui soit compatible avec leur ordre juridique interne.

Section 2 – Droit de procédure

131. Les articles de la présente Section décrivent certaines mesures de procédure à prendre au niveau national aux fins d'enquêtes pénales sur les infractions établies dans la Section 1, les autres infractions pénales commises au moyen d'un système informatique et la collecte de preuves sous forme électronique concernant une infraction pénale. En application du paragraphe 3 de l'article 39, aucune disposition de la Convention n'oblige ou n'invite une Partie à établir des pouvoirs ou des procédures autre que ceux énoncés dans la présente Convention, ni ne l'empêche de le faire.

132. La révolution technologique, qui englobe l'« inforoute » et ses nombreux types de communication et de services, interdépendants et interconnectés par la mise en commun des mêmes moyens et supports de transmission, a bouleversé le domaine du droit pénal et de la procédure pénale. La croissance ininterrompue des réseaux de communications ouvre de nouvelles perspectives à la criminalité, qu'il s'agisse des infractions classiques ou de la nouvelle criminalité technologique. Le droit pénal matériel ne doit pas se laisser distancer par ces actes illicites d'un type nouveau, mais cela est également vrai du droit pénal procédural et des techniques d'enquête. De la même façon, il y a lieu de prévoir et d'adapter des sauvegardes permettant d'avoir prise sur le nouvel environnement technologique et de développer de nouveaux pouvoirs de procédure.

133. L'un des problèmes les plus difficiles que pose la lutte contre la criminalité dans l'univers des réseaux est la difficulté d'identifier l'auteur d'une infraction

et d'évaluer la portée et l'impact de celle-ci. Un autre problème est lié à la volatilité des données électroniques, qui peuvent être modifiées, déplacées ou effacées en quelques secondes. Ainsi, par exemple, un utilisateur qui contrôle les données peut utiliser le système informatique pour effacer celles qui font l'objet d'une enquête pénale, détruisant ainsi toutes les preuves. La rapidité et, parfois, le secret sont souvent des ingrédients essentiels du succès d'une enquête.

134. La Convention adapte les procédures classiques telles que la perquisition et la saisie au nouveau milieu technologique. Parallèlement, de nouvelles mesures ont été mises en place, telles que la conservation rapide de données, de façon à s'assurer que les procédures classiques de collecte, comme la perquisition et la saisie, demeurent effectives dans un contexte technologique caractérisé par la volatilité. Les données n'étant pas toujours statiques, mais circulant dans le cadre du processus de communication, d'autres procédures classiques de collecte se rapportant aux télécommunications, telles que la collecte en temps réel de données de trafic et l'interception en temps réel des données de contenu, ont également été adaptées afin de rendre possible la collecte de données électroniques pendant le processus de communication lui-même. Certaines de ces procédures sont énoncées dans la Recommandation n° R (95) 13 du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information.

135. Toutes les dispositions dont il est question dans cette Section visent à permettre l'obtention ou la collecte de données aux fins des enquêtes ou des procédures pénales à mener. Les auteurs de la présente Convention ont examiné la question de savoir si celle-ci devrait imposer aux fournisseurs de services l'obligation de collecter et de conserver systématiquement les données de trafic pendant une période de temps déterminée, mais n'ont pas inséré une telle obligation car un consensus n'a pu être dégagé à ce sujet.

136. D'une manière générale, les procédures se rapportent à tous les types de données, y compris trois types spécifiques de données informatiques (données relatives au trafic, données relatives au contenu et les données relatives aux abonnés), qui peuvent se présenter sous deux formes (enregistrées ou en cours de transmission). On trouvera la définition de certains de ces termes aux articles 1 et 18. L'applicabilité d'une procédure à un type ou une forme particuliers de données électroniques dépend de la nature et de la forme des données et de la nature de la procédure, laquelle fait l'objet d'une description spécifique dans chaque article.

137. S'agissant d'adapter les procédures classiques au nouvel environnement technologique, la question de la terminologie appropriée se pose dans les dispositions de la présente section. On avait le choix entre conserver la terminologie classique (« perquisitionner » et « saisir »), utiliser des termes d'informatique nouveaux et plus proches du milieu technologique (« accéder » et « copier »), adoptés dans les textes d'autres instances internationales s'occupant du même sujet (comme le Sous-Groupe sur la criminalité de haute technologie du G8), ou retenir une solution de compromis (« perquisitionner ou accéder par un moyen similaire », et « saisir ou obtenir par un moyen similaire »). Comme il importe de tenir compte de l'évolution des concepts dans le milieu électronique tout en précisant et conservant leurs racines traditionnelles, on a retenu l'approche souple qui consiste à permettre aux Etats d'utiliser soit les notions classiques de « perquisition et saisie », soit les notions nouvelles d'« accès et copie ».

138. Tous les articles de cette Section font référence aux « autorités compétentes » et aux pouvoirs qui doivent leur être conférés aux fins des enquêtes ou procédures pénales. Dans certains pays, seuls les juges ont le pouvoir d'ordonner ou d'autoriser la collecte ou la production d'éléments de preuve, alors que, dans d'autres pays, les procureurs ou d'autres personnes chargées de veiller au respect de la loi sont investis de pouvoirs identiques ou similaires. Il s'ensuit que l'expression « autorité compétente » désigne une autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de procédures de collecte ou de production d'éléments de preuve se rapportant à des enquêtes ou procédures pénales.

Titre 1 – Dispositions communes

139. La Section s'ouvre sur deux dispositions de caractère général qui s'appliquent à tous les articles touchant le droit de procédure.

Champ d'application des mesures du droit de procédure (article 14)

140. Chaque Etat Partie est tenu d'adopter les mesures législatives et autres qui se révèlent nécessaires, conformément à son droit interne et à son cadre juridique, pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'« enquêtes ou de procédures pénales spécifiques. »

141. A deux exceptions près, chaque Partie applique les pouvoirs et procédures instaurés en application de la présente section: i) aux infractions

pénales établies conformément à la section 1 de la Convention ; ii) à toute autre infraction pénale commise au moyen d'un système informatique, et iii) à la collecte des preuves électroniques de toute infraction pénale. Ainsi, aux fins d'enquêtes ou de procédures pénales spécifiques, les pouvoirs et procédures mentionnés dans la présente section sont appliqués aux infractions établies conformément à la Convention, à toute autre infraction commise au moyen d'un système informatique et à la collecte des preuves électroniques de toute infraction pénale. De la sorte, les preuves électroniques de toute infraction pénale peuvent être obtenues ou collectées au moyen des pouvoirs et des procédures énoncés dans la présente section. On dispose ainsi de moyens d'obtention ou de collecte de données informatiques équivalents ou parallèles à ceux liés aux pouvoirs et procédures concernant les données non électroniques. La Convention indique clairement que les Parties devraient prévoir, dans leur droit interne, que des informations sous forme numérique ou sous une autre forme électronique peuvent servir de preuve devant une juridiction, dans le cadre d'une procédure pénale, quelle que soit la nature de l'infraction pénale faisant l'objet des poursuites.

142. Les procédures susvisées ne sont pas appliquées dans deux cas. Premièrement, l'article 21 dispose que le pouvoir d'intercepter des données relatives au contenu est limité à des infractions graves à définir dans le droit interne. Beaucoup d'Etats limitent le pouvoir d'interception des communications ou télécommunications orales aux infractions graves, eu égard au caractère confidentiel de ces communications ou télécommunications et du caractère interventionniste de cette mesure d'enquête. De même, la Convention n'impose aux Parties que d'établir des pouvoirs et procédures d'interception qu'en ce qui concerne des données relatives au contenu de communications informatiques spécifiées en relation avec des infractions graves à définir dans le droit interne.

143. Deuxièmement, une Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 (collecte en temps réel des données relatives au trafic) qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures d'interception mentionnées à l'article 21. Certains Etats considèrent que la collecte des données relatives au trafic est équivalente à la collecte des données relatives au contenu du point de vue du caractère confidentiel et interventionniste. Le droit de réserve permettrait à ces Etats de limiter l'application des mesures de collecte en temps réel des données

relatives au trafic au même éventail d'infractions auxquels ils appliquent les pouvoirs et procédures d'interception en temps réel des données relatives au contenu. Beaucoup d'Etats, toutefois, ne considèrent pas comme équivalentes l'interception des données relatives au contenu et la collecte des données relatives au trafic au regard des intérêts liés à la confidentialité et au degré d'interventionnisme, car la collecte des données relatives au trafic ne permet pas de collecter ou de divulguer le contenu de la communication. Etant donné que la collecte en temps réel de données relatives au trafic peut revêtir une très grande importance lorsqu'il s'agit de localiser la source ou la destination des communications informatiques (et, partant, d'identifier des malfaiteurs), la Convention invite les Parties qui exercent leur droit de réserve à limiter leur réserve de manière à permettre l'application la plus large possible des pouvoirs et procédures prévus pour collecter en temps réel des données relatives au trafic.

144. Le paragraphe (b) prévoit une possibilité de réserve pour les pays qui, en raison des restrictions déjà imposées par leur droit interne au moment de l'adoption de la Convention, ne sont pas en mesure d'intercepter des communications sur des systèmes informatiques mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé et qui n'utilisent pas les réseaux publics de télécommunications et ne sont pas non plus connectés à d'autres systèmes informatiques. L'expression « groupe d'utilisateurs fermé » fait référence par exemple à certains utilisateurs dont le nombre est limité par le fait qu'ils sont associés à un fournisseur de service, tels par exemple les employés d'une entreprise auxquels cette dernière fournit les moyens de communiquer entre eux par le biais d'un système informatique. L'expression « n'est pas connectée à un autre système informatique » signifie qu'au moment où un ordre prévu aux articles 20 et 21 serait émis, le système par le biais duquel les communications sont transmises n'a pas de connexion physique ou logique avec un autre système. L'expression « n'emploie pas les réseaux publics de télécommunications » exclut des systèmes qui utilisent des réseaux informatiques publics (y compris l'Internet), des réseaux téléphoniques publics ou d'autres moyens de télécommunications publics dans la transmission des communications, que cette utilisation soit ou non connue des utilisateurs.

Conditions et sauvegardes (article 15)

145. L'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section de la Convention doivent être sujettes aux conditions et sauvegardes prévues par le droit interne de chaque Partie.

Les Parties sont tenues d'instaurer certaines mesures relevant du droit de procédure dans leur droit interne, mais les modalités d'adoption et de mise en œuvre de ces pouvoirs et procédures dans le cadre de leur système juridique et l'application des pouvoirs et des procédures dans des cas spécifiques relèvent uniquement de la législation et des procédures internes de chaque Partie. Ces lois et procédures internes, telles que décrites plus en détail ci-après, doivent comprendre des conditions ou des sauvegardes, qui peuvent notamment être constitutionnelles, législatives ou fixées par le pouvoir judiciaire. Les modalités devraient prévoir en outre des éléments représentant des conditions et sauvegardes qui mettent en balance les impératifs de l'application de la loi et la défense des droits de l'homme et des libertés fondamentales. La Convention étant applicable à des Parties représentant un large éventail de systèmes et de cultures juridiques, il n'est pas possible de préciser en détail les conditions et sauvegardes applicables à chaque pouvoir ou procédure. Les Parties doivent veiller à ce que ces conditions et sauvegardes assurent une protection adéquate des droits de l'homme et des libertés fondamentales. Il existe certaines normes communes ou mesures minimales de sauvegarde auxquelles les Parties à la Convention doivent se conformer. Ces normes ou mesures minimales de sauvegarde sont généralement issues d'obligations que les Parties ont contractées en vertu des instruments internationaux relatifs aux droits de l'homme qui sont applicables. Il s'agit notamment de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et de ses Protocoles additionnels n°s 1, 4, 6, 7 et 12 (STE n° 005⁴, 009, 046, 114, 117 et 177), en ce qui concerne les Etats européens qui y sont Parties. Il s'agit aussi d'instruments applicables relatifs aux droits de l'homme auxquels sont parties des Etats situés dans d'autres régions du monde (la Convention américaine des droits de l'homme de 1969 et la Charte africaine des droits de l'homme et des peuples de 1981, par exemple), sans oublier le Pacte international relatif aux droits civils et politiques de 1966, qui a été ratifié par un bien plus

4. Le texte de la Convention avait été amendé conformément aux dispositions du Protocole n° 3 (STE n° 45), entré en vigueur le 21 septembre 1970, du Protocole n° 5 (STE n° 55), entré en vigueur le 20 décembre 1971, et du Protocole n° 8 (STE n° 118), entré en vigueur le 1^{er} janvier 1990, et comprenait en outre le texte du Protocole n° 2 (STE n° 44) qui, conformément à son article 5, paragraphe 3, avait fait partie intégrante de la Convention depuis son entrée en vigueur le 21 septembre 1970. Toutes les dispositions qui avaient été amendées ou ajoutées par ces Protocoles sont remplacées par le Protocole n° 11 (STE n° 155), à compter de la date de son entrée en vigueur, le 1^{er} novembre 1998. A compter de cette date, le Protocole n° 9 (STE n° 140), entré en vigueur le 1^{er} octobre 1994, est abrogé et le Protocole n° 10 (STE n° 146) est devenu sans objet.

grand nombre d'Etats. De plus, des protections analogues sont prévues par la législation de la plupart des Etats.

146. La Convention prévoit une autre mesure de sauvegarde en disposant que les pouvoirs et procédures doivent « intégrer le principe de proportionnalité ». Chaque Partie doit appliquer ce principe conformément aux autres principes pertinents de son droit interne. Pour les pays européens, il s'agira des principes issus de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), de sa jurisprudence applicable, ainsi que de la législation et de la jurisprudence nationales ; selon ces principes, les pouvoirs ou procédures doivent être proportionnels à la nature et aux circonstances de l'infraction. D'autres Etats mettront en œuvre des principes connexes de leur droit interne, tels que la limitation des injonctions de produire et les exigences de raisonnablement applicables aux perquisitions et saisies. Par ailleurs, la restriction expresse, à l'article 21, selon laquelle les obligations concernant les mesures d'interception sont limitées à un éventail d'infractions graves, définies par le droit interne, est un exemple clair de l'application du principe de proportionnalité.

147. Sans limiter les types de conditions et de sauvegardes qui pourraient être applicables, la Convention exige spécifiquement que ces conditions et sauvegardes comprennent – en fonction de la nature du pouvoir ou de la procédure – la supervision par une juridiction ou un autre organe indépendant, des motifs justifiant l'application du pouvoir ou de la procédure, et la limitation de sa portée ou de sa durée. Dans chaque pays, le législateur déterminera, en appliquant les obligations internationales incombant à l'Etat et les principes internes établis, quels pouvoirs et procédures constituent une ingérence suffisamment grave pour rendre nécessaire la mise en œuvre de conditions et de sauvegardes particulières. Ainsi que cela est indiqué au paragraphe 215, les Parties devraient en tout état de cause assortir l'interception – compte tenu de l'ingérence qu'elle constitue – de conditions et sauvegardes particulières. De telles sauvegardes ne doivent, par exemple, pas s'appliquer de manière identique à la conservation. Parmi les autres sauvegardes qui devraient être prévues par le droit interne figurent le droit de ne pas s'incriminer soi-même, la protection du secret professionnel et la prise en compte des caractéristiques des personnes ou des lieux auxquels s'applique une mesure donnée.

148. S'agissant des questions traitées au paragraphe 3, une grande importance doit être accordée à l'« intérêt public », et notamment une « bonne administration de la justice ». Dans la mesure où cela reste compatible avec l'intérêt public, les Parties devraient examiner d'autres facteurs, tels que l'impact du

pouvoir ou de la procédure sur « les droits, responsabilités et intérêts légitimes » de tiers, y compris les fournisseurs de services, qui découle des mesures de coercition, et les moyens pouvant être mis en œuvre pour réduire cet impact. En résumé, il faut d'abord prendre en compte la bonne administration de la justice et d'autres intérêts publics (comme par exemple la sécurité et la santé publiques, et d'autres intérêts, y compris les intérêts des victimes et le respect de la vie privée). Dans la mesure où cela reste compatible avec l'intérêt public, d'autres aspects devraient généralement être aussi pris en considération : réduire les perturbations dans la prestation de services aux consommateurs, faire en sorte que les personnes qui divulguent des données ou facilitent leur divulgation dans le cadre des dispositions du présent chapitre n'engagent pas leur responsabilité, ou protéger des intérêts patrimoniaux.

Titre 2 – Conservation rapide de données stockées

149. Les mesures mentionnées dans les articles 16 et 17 s'appliquent aux données stockées qui ont déjà été collectées et archivées par les détenteurs de données, tels que les fournisseurs de services. Elles ne s'appliquent pas à la collecte en temps réel et à la conservation de futures données relatives au trafic ni à l'accès en temps réel au contenu des communications. Ces questions sont traitées au Titre 5.

150. Les mesures décrites dans ces articles ne sont applicables que lorsque les données informatiques existent déjà et sont en cours de stockage. Il peut exister bien des raisons pour lesquelles les données informatiques présentant un intérêt pour les enquêtes pénales n'existent pas ou ne sont plus stockées. Ainsi, par exemple, on peut n'avoir ni collecté ni conservé des données exactes ou, si on en a collecté, on ne les a pas conservées. Les lois régissant la protection des données peuvent avoir imposé la destruction de données importantes avant que qui que ce soit ne réalise leur importance pour la procédure pénale. Parfois, il n'existe pas de motif commercial pour collecter et conserver des données, comme dans le cas où les clients paient un tarif forfaitaire pour des services ou que les services sont gratuits. Les articles 16 et 17 n'abordent pas ces problèmes.

151. Il importe d'établir une distinction entre la « conservation des données » et l'« archivage des données ». Les deux expressions ont des sens voisins dans le langage courant, mais différents en informatique. Conserver des données, c'est garder des données qui existent déjà sous une forme stockée et en les protégeant contre tout ce qui pourrait en altérer ou en dégrader la qualité ou l'état actuel. Archiver des données, c'est garder en sa possession pour l'avenir

des données qui sont en cours de production. L'archivage des données implique l'accumulation des données dans le présent et la garde ou la possession de ces données en prévision d'une période future. L'archivage des données est le processus de stockage des données. En revanche, la conservation des données est l'activité qui garantit leur sécurité et leur sûreté.

152. Les articles 16 et 17 ne concernent que la conservation des données, non leur archivage. Ils ne prescrivent pas la collecte et l'archivage de l'ensemble, voire d'une partie des données collectées par un fournisseur de services ou une autre entité dans le cadre de ses activités. Les mesures de conservation s'appliquent aux données électroniques « *stockées* au moyen d'un système informatique », ce qui suppose que les données existent déjà, ont déjà été collectées et sont stockées. De plus, comme l'indique l'article 14, tous les pouvoirs et procédures devant être instaurés en application de la section 2 de la Convention doivent l'être « aux fins d'enquêtes ou de procédures pénales spécifiques », ce qui restreint l'application des mesures à une enquête concernant une affaire donnée. En outre, lorsqu'une partie applique les mesures de conservation au moyen d'une ordonnance, celle-ci porte sur « des données stockées spécifiées se trouvant en la possession ou sous le contrôle de la personne » (paragraphe 2 de l'article 16). Les articles 16 et 17 prévoient donc uniquement le pouvoir de requérir la conservation de données stockées existantes, en attendant la divulgation des données en application d'autres pouvoirs juridiques, à l'occasion d'enquêtes ou de procédures pénales spécifiques.

153. L'obligation d'assurer la conservation des données ne consiste pas à requérir des Parties qu'elles limitent l'offre ou l'utilisation de services qui ne s'emploient pas systématiquement à collecter et archiver certains types de données, telles que les données relatives au trafic ou aux abonnés, dans le cadre de leurs pratiques commerciales légitimes. Elle ne consiste pas non plus à imposer aux Parties de mettre en œuvre à cette fin de nouvelles possibilités techniques, par exemple pour conserver des données éphémères qui ne restent dans le système que pour une durée si brève qu'elles ne peuvent raisonnablement être conservées en réponse à une demande ou à une injonction.

154. Dans certains Etats, la loi requiert que certains types de données, telles que les données personnelles, en la possession de certaines catégories de détenteurs ne soient pas archivées, mais effacées lorsque leur archivage ne répond plus à une fin commerciale. Dans l'Union européenne, le principe général est mis en pratique par la Directive 95/46/EC et, dans le contexte particulier du secteur des télécommunications, par la Directive 97/66/EC. Ces directives instaurent l'obligation d'effacer les données dès que leur stockage

n'est plus nécessaire. Toutefois, les Etats membres peuvent adopter une législation prévoyant des dérogations lorsqu'elles sont nécessaires pour prévenir la commission d'infractions pénales, instruire les infractions ou poursuivre leurs auteurs. Ces directives n'empêchent pas les Etats membres de l'Union européenne d'instaurer des pouvoirs et procédures en droit interne pour conserver des données spécifiées aux fins d'enquêtes spécifiques.

155. Pour la plupart des pays, la conservation des données constitue un pouvoir ou une procédure juridique entièrement nouveau en droit interne. Il s'agit d'un nouvel instrument d'enquête important dans la lutte contre la criminalité informatique et en relation avec l'ordinateur, en particulier contre les infractions commises par le biais de l'Internet. Premièrement, en raison de leur volatilité, les données informatiques sont faciles à manipuler et à modifier. Ainsi, il est facile de perdre des éléments prouvant une infraction si les pratiques de traitement et de stockage manquent de rigueur, si les données sont intentionnellement manipulées ou effacées pour détruire tout élément de preuve ou si elles sont effacées dans le cadre d'opérations normales d'effacement de données qui n'ont plus à être conservées. L'un des moyens de préserver l'intégrité des données consiste pour les autorités compétentes à opérer des perquisitions ou à accéder d'une autre manière aux données et à saisir les données ou à se les procurer d'une autre manière. Toutefois, lorsque le gardien des données est digne de confiance, comme dans le cas d'une entreprise ayant une bonne réputation, l'intégrité des données peut être garantie plus rapidement au moyen d'une injonction de conserver les données. Une injonction d'avoir à conserver les données peut être moins perturbatrice pour les activités et moins préjudiciable à la réputation d'une entreprise honnête qu'une opération de perquisition de ses locaux aux fins de saisie. Deuxièmement, les infractions informatiques et en relation avec l'ordinateur sont très souvent commises au moyen de la transmission de communications par le biais du système informatique. Ces communications peuvent contenir un contenu illicite, tel que la pornographie infantile, des virus informatiques ou d'autres instructions qui portent atteinte aux données ou entravent le bon fonctionnement du système informatique, ou des éléments tendant à prouver que d'autres infractions ont été commises, par exemple des cas de trafic de stupéfiants ou d'escroquerie. L'identification de la source ou de la destination de ces communications antérieures peut aider à établir l'identité des auteurs de ces infractions. Pour déterminer la source ou la destination de ces communications, il faut disposer de données relatives au trafic concernant ces communications antérieures (pour d'autres explications sur l'importance des données relatives au trafic, se reporter à l'article 17 ci-dessous).

Troisièmement, lorsque ces communications présentent un contenu illicite ou la preuve d'agissements criminels et que des copies de ces communications sont archivées par les fournisseurs de services (de courrier électronique, par exemple), la conservation de ces communications est importante afin de ne pas perdre des éléments de preuve essentiels. L'obtention de copies de ces communications antérieures (par exemple de courriers stockés qui ont été envoyés ou reçus) peut révéler que des infractions ont été commises.

156. Le pouvoir de conservation rapide des données informatiques doit permettre de faire face à ces problèmes. Les Parties sont donc invitées à instaurer le pouvoir d'ordonner la conservation de données informatiques spécifiées, en tant que mesure provisoire ; les données seront conservées durant une période aussi longue que nécessaire, qui pourra aller jusqu'à 90 jours. Les Parties pourront prévoir le renouvellement de cette mesure. Durant la période de conservation, les données ne sont pas automatiquement portées à la connaissance des services répressifs. En effet, pour que les données puissent être divulguées, il faut prendre une mesure supplémentaire de divulgation ou ordonner une perquisition. A propos de la communication de données conservées aux services répressifs, voir les paragraphes 152 et 160.

157. Il importe tout autant que des mesures de conservation soient en place au niveau national afin de permettre aux Parties de se porter assistance au niveau international en ce qui concerne la conservation rapide de données stockées sur leur territoire. On peut ainsi s'assurer que des données essentielles ne disparaissent pas pendant la longue procédure d'entraide judiciaire classique pendant laquelle la Partie requise se procure les données et les remet à la Partie requérante.

Conservation rapide de données stockées dans un système informatique (article 16)

158. L'article 16 vise à donner aux autorités nationales compétentes la possibilité d'ordonner ou d'obtenir par un moyen similaire la conservation rapide de données électroniques stockées spécifiées dans le cadre d'une enquête ou d'une procédure pénale spécifique.

159. La « conservation » exige que les données qui existent déjà et sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou dégrader la qualité ou l'état actuel. Elle exige que les données soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient « gelées »

(c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes. La personne à laquelle est adressée l'injonction peut, en fonction des spécifications exactes de celle-ci, conserver l'accès aux données. L'article ne précise pas la manière dont les données doivent être conservées. Il appartient à chaque Partie d'établir les modalités appropriées de conservation et de déterminer si, dans certains cas, la conservation des données devrait également comporter le « gel » de celles-ci.

160. La mention « ordonner ou ... obtenir par un moyen similaire » vise à autoriser la mise en œuvre d'autres moyens juridiques de conservation que l'injonction judiciaire ou administrative ou une instruction (de la police ou du parquet, par exemple). Dans certains Etats, le droit de procédure ne prévoit pas d'injonctions de conservation ; les données ne peuvent alors être conservées que par la voie d'opérations de perquisition et saisie ou d'une injonction de produire. L'utilisation du membre de phrase « ou ... obtenir par un moyen similaire » introduit la souplesse voulue pour permettre à ces Etats d'appliquer cet article en mettant en œuvre ces autres moyens. Toutefois, il est recommandé aux Etats d'envisager d'instaurer des pouvoirs et procédures permettant d'ordonner effectivement au destinataire d'une injonction de conserver les données, car la rapidité de l'intervention de cette personne peut, dans certains cas, permettre d'appliquer plus rapidement les mesures de conservation.

161. Le pouvoir d'ordonner ou d'obtenir d'une autre manière la conservation rapide de données électroniques spécifiées s'applique à tout type de données informatiques stockées. Il peut s'agir de tout type de données qui est spécifié dans l'ordre de conserver, comme des dossiers commerciaux, médicaux ou personnels. Les Parties doivent instaurer ces mesures pour les appliquer « notamment lorsqu'il y a des raisons de penser que [les données] sont particulièrement susceptibles de perte ou de modification. » Il peut se faire, par exemple, que les données ne soient archivées que pour une brève période. C'est le cas, par exemple, lorsqu'une entreprise a pour politique d'effacer les données au bout d'un certain temps ou que les données sont systématiquement effacées lorsque le support de stockage est utilisé pour enregistrer d'autres données. Le risque peut également tenir aux caractéristiques du gardien des données ou au fait que les données sont stockées d'une manière qui n'en garantit pas la protection. Toutefois, si le gardien n'était pas digne de confiance, il serait plus sûr de procéder à la conservation par perquisition et saisie plutôt que par une injonction à laquelle l'intéressé pourrait ne pas

obtempérer. Le paragraphe 1 mentionne expressément les « données relatives au trafic » afin d'indiquer l'applicabilité particulière de ces dispositions à ce type de données, lesquelles, lorsqu'elles sont collectées et archivées par un fournisseur de services, ne sont généralement conservées que une brève période. Par ailleurs, la mention des « données relatives au trafic » établit un lien entre les mesures visées aux articles 16 et 17.

162. Le paragraphe 2 précise que, lorsqu'une Partie applique la mesure de conservation en adressant une injonction de conserver, celle-ci porte sur des « données stockées spécifiées se trouvant en la possession ou sous le contrôle de [la personne à laquelle l'injonction est adressée] ». Ainsi les données stockées peuvent-elles être effectivement en la possession de l'intéressé ou peuvent être stockées ailleurs tout en étant placées sous son contrôle. La personne qui reçoit l'injonction est obligée de « conserver et protéger l'intégrité de ces données pendant une durée aussi longue que nécessaire, jusqu'à un maximum de 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. » Le droit interne de chaque Partie devrait instituer une durée maximale pendant laquelle les données faisant l'objet d'une injonction doivent être conservées et l'injonction devrait spécifier la durée exacte pendant laquelle les données spécifiées doivent être conservées. La durée, qui ne devrait pas excéder 90 jours, devrait être suffisante pour permettre aux autorités compétentes de prendre d'autres mesures juridiques, telles que la perquisition et la saisie, l'accès aux données ou leur obtention par un moyen similaire, ou l'émission d'une injonction de produire, en vue d'obtenir la divulgation des données. Les Parties pourront prévoir le renouvellement de l'injonction de produire. A cet égard, on se reportera à l'article 29, qui porte sur une demande d'entraide aux fins d'obtenir la conservation rapide de données stockées au moyen d'un système informatique. Cet article précise que la conservation effectuée en réponse à une demande d'entraide « sera valable pour une période d'au moins 60 jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'acquisition par un moyen similaire, ou de la divulgation des données. »

163. Le paragraphe 3 impose une obligation de confidentialité sur la mise en œuvre des procédures de conservation au gardien des données ou à une autre personne à qui il est enjoint de conserver celles-ci pendant la durée prévue par son droit interne. Les Parties sont ainsi tenues d'instaurer des mesures de confidentialité concernant la conservation rapide de données stockées ainsi qu'une durée maximale de confidentialité. Cette mesure tient compte des besoins de la lutte contre la criminalité en faisant en sorte que le suspect

faisant l'objet d'une enquête n'ait pas connaissance de celle-ci, ainsi que du droit des particuliers au respect de leur vie privée. Pour les services de lutte contre la criminalité, la conservation rapide des données s'inscrit dans le cadre des enquêtes préliminaires, période durant laquelle il peut être important de conserver le secret. La conservation est une mesure préliminaire adoptée en attendant que soient prises d'autres mesures juridiques visant à obtenir les données ou leur divulgation. La confidentialité s'impose pour éviter que d'autres personnes ne tentent de manipuler ou d'effacer les données. Pour la personne à laquelle l'injonction est adressée, la personne concernée ou d'autres personnes pouvant être mentionnées ou identifiées dans les données, la durée maximale de la mesure est bien spécifiée. La double obligation de garantir la sécurité des données et de s'assurer que le secret sur la mise en œuvre de la mesure de conservation est gardé contribue à défendre le droit à la vie privée de la personne concernée ou des autres personnes pouvant être mentionnées ou identifiées dans ces données.

164. En sus des limitations précitées, les pouvoirs et procédures mentionnés dans l'article 16 doivent être soumis aux conditions et sauvegardes prévues aux articles 14 et 15.

Conservation et divulgation rapides de données relatives au trafic (article 17)

165. Cet article instaure des obligations spécifiques concernant la conservation des données relatives au trafic visées à l'Article 16 et prévoit la divulgation rapide de certaines données relatives au trafic aux fins d'identification des autres fournisseurs de services ayant participé à la transmission de communications spécifiées. Les « données relatives au trafic » sont définies à l'article premier.

166. L'obtention de données relatives au trafic stockées concernant des communications antérieures peut être indispensable pour déterminer la source ou la destination de ces communications, ce qui est essentiel pour identifier les personnes qui, par exemple, ont distribué de la pornographie enfantine, diffusé de fausses déclarations dans le cadre d'une manœuvre frauduleuse, propagé des virus informatiques, tenté d'accéder de façon illicite à des systèmes informatiques ou réussi à le faire, ou transmis à un système informatique des communications qui ont soit porté atteinte aux données du système, soit entravé le bon fonctionnement de celui-ci. Or, ces données ne sont souvent stockées que pour une courte durée, la législation protégeant le droit au respect de la vie privée pouvant interdire le stockage de longue durée de ces données quand ce ne sont pas les forces de marché qui le découragent.

Il est donc important de mettre en œuvre des mesures de conservation pour garantir l'intégrité de ces données (on se reportera à l'analyse de la question de la conservation ci-dessus).

167. Il arrive souvent que plusieurs fournisseurs de services participent à la transmission d'une communication. Chaque fournisseur peut posséder certaines données relatives au trafic concernant la transmission de la communication spécifiée, qui ont soit été produites et archivées par ce fournisseur à l'occasion du passage de la communication par son système, soit ont été fournies par d'autres fournisseurs. Il arrive que les données relatives au trafic, ou tout au moins certains types de données relatives au trafic, soient partagées entre les fournisseurs de services ayant participé à la transmission de la communication, à des fins commerciales, sécuritaires ou techniques. En pareil cas, l'un ou l'autre de ces fournisseurs peut posséder les données relatives au trafic essentielles pour déterminer la source ou la destination de la communication. Souvent, toutefois, aucun fournisseur ne possède à lui seul suffisamment de données relatives au trafic pour permettre de déterminer avec exactitude la source ou la destination de la communication. Chacun possède certaines parties du puzzle et chacune de ces parties doit être examinée afin d'identifier la source ou la destination.

168. L'article 17 veille, lorsqu'un seul ou plusieurs fournisseurs de services ont participé à la transmission d'une communication, à ce qu'il soit procédé à la conservation rapide des données relatives au trafic parmi tous les fournisseurs. Il ne précise pas les moyens d'y parvenir, laissant au droit interne le soin de déterminer un moyen compatible avec l'ordre juridique et économique national. Un moyen de procéder à la conservation rapide consisterait pour les autorités compétentes à adresser rapidement une injonction distincte à chacun des fournisseurs de services. Mais l'obtention de plusieurs injonctions distinctes peut demander beaucoup trop de temps. Une solution à préférer serait d'obtenir une injonction unique mais qui s'appliquerait à tous les fournisseurs identifiés ultérieurement comme ayant participé à la transmission de la communication spécifiée. Cette injonction générale pourrait être notifiée successivement à chacun des fournisseurs identifiés. On pourrait également solliciter la participation des fournisseurs. On pourrait, par exemple, demander à un fournisseur ayant reçu une injonction de transmettre au fournisseur occupant le maillon suivant de la chaîne l'existence et la teneur de cette injonction de conservation. Cette transmission pourrait, selon les dispositions du droit interne, avoir pour effet soit d'autoriser le deuxième fournisseur à conserver volontairement les données relatives au trafic pertinentes, et ce en dépit de

toutes obligations préexistantes selon lesquelles il serait tenu de les effacer, soit de rendre obligatoire cette conservation. Le deuxième fournisseur pourrait de son côté répercuter la teneur de l'injonction au fournisseur occupant le maillon suivant de la chaîne.

169. Comme les données relatives au trafic ne sont pas divulguées aux autorités répressives au moment où une injonction de conserver est adressée à un fournisseur de services (mais seulement obtenues ou divulguées par la suite, au moment de la prise des autres mesures juridiques), ces autorités ne savent pas si le fournisseur en question possède toutes les données relatives au trafic essentielles ou si d'autres fournisseurs ont participé à la transmission de la communication. Aussi cet article impose-t-il que le fournisseur de services qui a reçu l'ordre de conservation divulgue rapidement aux autorités compétentes, ou à une autre personne désignée par celles-ci, une quantité suffisante de données relatives au trafic aux fins d'identification de tous autres fournisseurs de services et de la voie par laquelle la communication a été transmise. Les autorités compétentes devraient préciser clairement le type de données relatives au trafic qu'il importe de divulguer. L'obtention de cette information permettrait aux autorités compétentes de décider si elles doivent prendre des mesures de conservation vis-à-vis des autres fournisseurs. De la sorte, les autorités chargées d'une enquête peuvent déterminer l'origine ou la destination de la communication et identifier l'auteur ou les auteurs de l'infraction spécifique faisant l'objet de l'enquête. Les mesures mentionnées dans cet article doivent également être soumises aux limitations, conditions et sauvegardes visées aux articles 14 et 15.

Titre 3 – Injonction de produire

Injonction de produire (article 18)

170. Au paragraphe 1 de cet article, les Parties sont invitées à habiliter leurs autorités compétentes à contraindre une personne présente sur leur territoire à fournir des données informatiques stockées spécifiées ou un fournisseur de services offrant ceux-ci sur le territoire d'une Partie à communiquer les données relatives à l'abonné. Les données en question sont des données stockées ou existantes et n'englobent pas les données qui n'existent pas encore, comme les données relatives au trafic ou au contenu se rapportant aux communications futures. Au lieu de requérir des Etats qu'ils appliquent systématiquement des mesures contraignantes à l'égard de tiers, telles que la perquisition et la saisie de données, il est essentiel que les Etats disposent

dans leur droit interne d'autres pouvoirs d'enquête qui leur donnent un moyen moins intrusif d'obtenir des informations utiles pour les enquêtes pénales.

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

172. L'injonction de produire porte sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services.

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, doit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Dans certains Etats, la notion juridique de « possession » recouvre la possession matérielle et de droit de manière assez large pour satisfaire à cette exigence de « possession ou de contrôle ».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de « communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services ». De même qu'au paragraphe 1(a), l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression « qui se rapportent à ces services » signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction.

174. Les conditions et sauvegardes visées au paragraphe 2 de l'article peuvent, en fonction du droit interne de chaque Partie, exclure des données ou informations confidentielles. Une Partie pourra prescrire des choix différents concernant les conditions, les autorités compétentes et les sauvegardes à propos de la communication de tel ou tel type de données informatiques ou de données relatives à l'abonné détenues par telle ou telle catégorie de personnes ou de fournisseurs de services. Ainsi, par exemple, en ce qui concerne certains types de données telles que les données relatives à l'abonné connues de tous, une Partie pourra habilitier les agents de la force publique à émettre une injonction de ce genre tandis qu'une ordonnance d'un tribunal pourrait être requise dans d'autres situations. En revanche, dans certaines situations, une Partie pourrait exiger ou se voir imposer par des sauvegardes relevant des droits de l'homme d'exiger qu'une injonction de produire soit émise uniquement par une autorité judiciaire afin de pouvoir obtenir certains types de données. Les Parties pourraient souhaiter limiter la divulgation de ces données aux fins de lutte contre la criminalité aux situations dans lesquelles une injonction de produire en vue de la divulgation de ces données a été rendue par une autorité judiciaire. Par ailleurs, le principe de proportionnalité introduit une certaine souplesse dans l'application de la mesure, par exemple en l'excluant dans les affaires sans gravité.

175. Les Parties peuvent également envisager d'instaurer des mesures relatives à la confidentialité. L'article ne mentionne pas spécifiquement la confidentialité, ceci afin de préserver le parallélisme avec le monde non électronique, où la confidentialité n'est en général pas imposée en ce qui concerne les injonctions de produire. Toutefois, dans le monde électronique, et en particulier le monde

en ligne, une injonction de produire peut parfois servir de mesure préliminaire dans le cadre d'une enquête, précédant d'autres mesures telles que la perquisition et la saisie ou l'interception en temps réel d'autres données. Le succès de l'enquête pourrait dépendre de la confidentialité.

176. S'agissant des modalités de production, les Parties peuvent instaurer l'obligation de produire des données informatiques ou des informations relatives à l'abonné de la manière spécifiée dans l'injonction. Elles pourraient ainsi mentionner le délai dans lequel la divulgation doit intervenir ou la forme sous laquelle les données doivent être divulguées (« texte en clair », en ligne, sortie imprimée ou disquette).

177. L'expression « informations relatives aux abonnés » est définie au paragraphe 3. En principe, elle désigne toute information détenue par l'administration d'un fournisseur de services et qui se rapporte à un abonné à ses services. Les données relatives aux abonnés peuvent être contenues sous forme de données informatiques ou sous toute autre forme, telle que des documents-papier. Comme les informations relatives aux abonnés ne se présentent pas toutes sous la forme de données informatiques, une disposition spéciale a été insérée dans l'article pour tenir compte de ce type d'informations. Le terme d'« abonné » vise à englober de nombreuses catégories de clients des fournisseurs de services : personne ayant payé un abonnement, client qui paie au fur et à mesure les services qu'il utilise, personne bénéficiant de services gratuits. Sont aussi incluses les informations concernant les personnes habilitées à utiliser le compte de l'abonné.

178. Dans le cadre d'une enquête pénale, les informations relatives aux abonnés peuvent être nécessaires dans deux situations spécifiques. Premièrement, elles sont nécessaires pour déterminer les services et mesures techniques connexes qui ont été utilisés ou sont utilisés par un abonné, tels que le type de service téléphonique utilisé (par exemple téléphonie mobile), le type de services connexes utilisé (renvoi automatique d'appel, messagerie téléphonique, etc.), le numéro de téléphone ou toute autre adresse technique (comme une adresse électronique). Deuxièmement, lorsqu'une adresse technique est connue, les informations relatives aux abonnés sont requises pour aider à établir l'identité de l'intéressé. D'autres informations relatives aux abonnés, telles que les informations commerciales figurant dans les dossiers de facturation et de paiement de l'abonné, peuvent également être utiles aux enquêtes pénales surtout lorsque l'infraction faisant l'objet de l'enquête concerne un cas de fraude informatique ou un autre délit économique.

179. En conséquence, les informations relatives aux abonnés recouvrent différents types d'informations sur l'utilisation d'un service et l'utilisateur de ce service. S'agissant de l'utilisation du service, l'expression désigne toute information, autre que des données relatives au trafic ou au contenu, permettant d'établir le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période pendant laquelle l'intéressé a été abonné au service en question. L'expression « dispositions techniques » désigne l'ensemble des mesures prises pour permettre à l'abonné de profiter du service de communication offert. Ces dispositions incluent notamment la réservation d'un numéro ou adresse technique (numéro de téléphone, adresse de site Web ou nom de domaine, adresse électronique, etc.) ainsi que la fourniture et l'enregistrement du matériel de communication utilisé par l'abonné (appareils de téléphonie, centres d'appel ou réseaux locaux).

180. Les informations relatives aux abonnés ne sont pas limitées aux informations se rapportant directement à l'utilisation du service de communication. Elles désignent également toutes les informations, autres que des données relatives au trafic ou au contenu, qui permettent d'établir l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'utilisateur, et tout autre numéro d'accès et les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou arrangement de service entre l'abonné et le fournisseur de services. Elles désignent en outre toute autre information, autre que des données relatives au trafic ou au contenu, relative à l'endroit où se trouvent les équipements de communication, information disponible sur la base d'un contrat ou arrangement de service. Cette dernière information peut n'avoir d'intérêt pratique que dans le cas d'équipements non portatifs, mais le fait de savoir si les équipements en question sont portatifs ou de connaître l'endroit où ils se trouveraient (sur la base de l'information fournie en vertu du contrat ou de l'arrangement de service) peut être utile à l'enquête.

181. Cet article ne fait toutefois pas obligation aux fournisseurs de services de conserver des données sur leurs abonnés. Et les fournisseurs ne seront pas non plus tenus, en vertu de la Convention, de s'assurer de l'exactitude desdites données. En d'autres termes, les fournisseurs de services ne sont pas astreints à enregistrer les données relatives à l'identité des utilisateurs des télécartes donnant accès aux services radiotéléphoniques mobiles. Ils ne sont pas non plus obligés de vérifier l'identité des abonnés ou de s'opposer à l'emploi de pseudonymes par les utilisateurs de leurs services.

182. Les pouvoirs et procédures faisant l'objet de la présente section étant instaurés aux fins d'enquêtes ou de procédures pénales spécifiques (article 14),

les injonctions de produire sont appelées à être utilisées dans des affaires individuelles concernant le plus souvent un abonné. Ainsi, par exemple, sur la base de la mention du nom de telle ou telle personne dans l'injonction de produire, un numéro de téléphone ou une adresse électronique peuvent être demandés. Sur la base d'un certain numéro de téléphone ou d'une certaine adresse électronique, le nom et l'adresse de l'abonné peuvent être demandés. La mention susvisée n'autorise pas les Parties à rendre une ordonnance aux fins de divulgation de quantités non sélectives d'informations relatives aux abonnés par un fournisseur de services relatives à des groupes d'abonnés, par exemple aux fins d'extraction de données.

183. La mention d'un « contrat ou arrangement de service » s'entend au sens très large de tout type de relation sur la base duquel un abonné utilise les services d'un fournisseur.

Titre 4 – Perquisition et saisie de données informatiques stockées

Perquisition et saisie de données informatiques stockées (article 19)

184. Cet article vise à moderniser et harmoniser les législations internes concernant la perquisition et la saisie de données informatiques stockées aux fins de recueillir des preuves se rapportant à des enquêtes ou procédures pénales spécifiques. Toute législation interne relative à la procédure pénale prévoit des pouvoirs de perquisition et de saisie d'objets tangibles. Toutefois, dans plusieurs Etats, les données informatiques stockées ne sont pas considérées en soi comme des choses tangibles et ne peuvent donc pas être obtenues aux fins d'une enquête ou d'une procédure pénale de la même façon que des objets tangibles, à moins d'appréhender le support sur lequel ces données sont stockées. L'objectif de l'article 19 de la Convention est d'établir un pouvoir équivalent relatif aux données stockées.

185. Dans le cadre de la perquisition classique portant sur des documents ou des dossiers, une perquisition consiste à recueillir des informations qui ont été consignées ou enregistrées dans le passé sous une forme matérielle, comme celles couchées à l'encre sur du papier. Les enquêteurs perquisitionnent ou inspectent ces données ainsi enregistrées et saisissent ou emportent physiquement des dossiers tangibles. La collecte des données a lieu pendant la perquisition et porte sur les données existant à ce moment-là. La condition à remplir pour obtenir l'autorisation légale de procéder à une perquisition est l'existence, en vertu de la législation interne et des dispositions relatives à la défense des droits de l'homme, de raisons de penser que de telles données

existent dans un endroit précis et permettront de prouver qu'une infraction pénale spécifique a été commise.

186. S'agissant de la recherche d'informations, en particulier de données informatiques, beaucoup d'éléments de la perquisition classique subsistent dans le nouvel environnement technologique. Ainsi, par exemple, la collecte des données a lieu pendant la perquisition et porte sur les données existant à ce moment-là. Les conditions à remplir pour obtenir l'autorisation légale de procéder à une perquisition demeurent les mêmes. Le degré de conviction requis pour obtenir cette autorisation légale de perquisition ne dépend pas de la forme, tangible ou électronique, sous laquelle se présentent les données en question. De même, la conviction et la perquisition concernent des données qui existent déjà et qui permettront d'établir qu'une infraction spécifique a été commise.

187. Toutefois, en ce qui concerne la recherche de données informatiques, des dispositions procédurales supplémentaires sont nécessaires pour garantir que l'obtention des données informatiques puisse se faire d'une manière aussi efficace que la perquisition et la saisie de supports d'information tangibles. Cela s'explique par plusieurs raisons. Premièrement, les données se présentent sous une forme intangible, par exemple électromagnétique. Deuxièmement, les données peuvent être lues à l'aide d'un matériel informatique, mais ne peuvent pas être saisies et emportées de la même façon qu'un document-papier. Le support matériel sur lequel les données intangibles sont stockées (qui peut être le disque dur d'un ordinateur ou une disquette) doit être saisi et emporté ou une copie des données doit être faite sous forme soit tangible (copie papier, par exemple), soit intangible sur un support matériel (comme une disquette), avant que le support tangible contenant la copie ne puisse être saisi et emporté. Dans les deux dernières situations, donnant lieu à la copie des données, les données originelles restent dans le système informatique ou le dispositif de stockage (mémoire). La législation interne devrait instaurer le pouvoir de faire de telles copies. Troisièmement, du fait de la connectivité des systèmes informatiques, les données peuvent ne pas être stockées dans l'ordinateur faisant l'objet de la perquisition, mais elles peuvent être facilement accessibles par ce système. Elles pourraient être stockées dans un dispositif de stockage associé directement connecté à l'ordinateur ou connecté indirectement à l'ordinateur via des systèmes de communications tels que l'internet. Ce fait peut ou non imposer l'adoption de lois nouvelles autorisant l'extension de la perquisition à l'endroit où les données sont effectivement stockées (ou le rapatriement des données de l'endroit en question pour les transférer

à l'ordinateur faisant l'objet de la perquisition), ou l'utilisation de pouvoirs de perquisition classique d'une manière mieux coordonnée et plus rapide aux deux endroits.

188. Le paragraphe 1 oblige les Parties à habiliter leurs autorités chargées de la lutte contre la criminalité à perquisitionner et à accéder aux données informatiques contenues soit dans un système informatique, soit dans une partie de celui-ci (qui peut être un dispositif de stockage connecté), ou sur un support de stockage indépendant (tel qu'un CD-ROM ou une disquette). Etant donné qu'en application de l'article 1, l'expression «système informatique» désigne «tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés», le paragraphe 1 concerne la perquisition d'un système informatique et de ses composants apparentés pouvant être considérés comme constituant ensemble un système informatique distinct (c'est le cas, par exemple, d'un ordinateur portable et de l'imprimante et des dispositifs de stockage apparentés, ou d'un réseau local). Parfois, des données stockées physiquement dans un autre système ou dans un dispositif de stockage sont accessibles légalement par le biais du système informatique perquisitionné en établissant une connexion avec d'autres systèmes informatiques distincts. Cette situation, qui implique le raccordement à d'autres systèmes informatiques au moyen de réseaux de télécommunications à l'intérieur du même territoire (réseau étendu ou Internet) est abordé au paragraphe 2.

189. L'opération de perquisition et saisie d'un «support de stockage informatique permettant de stocker des données informatiques» [paragraphe 1 b)] peut être effectuée en se prévalant de pouvoirs de perquisition classiques, mais l'application d'une mesure de perquisition informatique exige souvent la perquisition tant du système informatique que de tout support de stockage apparenté (comme des disquettes) se trouvant dans le voisinage immédiat du système informatique. Du fait de ce lien entre les deux, le paragraphe 1 prévoit une habilitation globale couvrant les deux situations.

190. L'article 19 s'applique aux données informatiques stockées. A cet égard, la question est de savoir si un courrier non ouvert, qui attend dans la boîte aux lettres d'un fournisseur de services Internet que le destinataire le télécharge sur son système informatique, doit être considéré comme des données informatiques stockées ou des données en cours de transmission. En vertu de la législation de certaines Parties, ce courrier fait partie d'une communication, et son contenu ne peut donc être obtenu qu'au moyen du pouvoir d'interception alors que, dans d'autres systèmes juridiques, ce courrier est assimilé à des données stockées auxquelles s'applique l'article 19. En conséquence,

les Parties devraient examiner leur législation concernant cette question pour déterminer les dispositions de leur ordre juridique interne à appliquer en l'espèce.

191. Le paragraphe utilise l'expression « perquisitionner ou ... accéder par un moyen similaire ». L'emploi du mot classique « perquisitionner » traduit l'idée de l'exercice par l'Etat d'un pouvoir coercitif et montre que le pouvoir visé dans cet article est analogue à la perquisition classique. « Perquisitionner » veut dire rechercher, lire, inspecter ou examiner des données, et inclut aussi les notions de recherche de données et d'examen de données. En revanche, le mot « accéder » a un sens neutre, mais est plus fidèle à la terminologie informatique. Les deux termes sont utilisés pour combiner les notions classiques et la terminologie moderne.

192. L'expression « sur son territoire » sert à rappeler que cette disposition, comme tous les articles de cette section, ne concerne que les seules mesures qui doivent être prises au niveau national.

193. Le paragraphe 2 habilite les autorités chargées d'une enquête à étendre l'opération entreprise pour perquisitionner ou accéder par un moyen similaire à un autre système informatique ou une partie de celui-ci lorsqu'elles ont des raisons de penser que les données sollicitées sont stockées dans cet autre système informatique. Cet autre système informatique ou la partie de ce système ainsi perquisitionnée doit toutefois se trouver également « sur son territoire ».

194. La Convention ne prescrit pas les modalités d'autorisation ni d'application de l'extension de la mesure de perquisition. C'est à la législation interne qu'il appartient de les fixer. On peut citer quelques exemples d'options possibles : habiliter l'autorité, judiciaire ou autre, qui a autorisé la perquisition d'un système informatique donné à autoriser également l'extension de la perquisition ou du moyen d'accès similaire à un système connecté si elle a des raisons de penser (dans la mesure exigée par la législation nationale et les dispositions relatives à la défense des droits de l'homme) que le système informatique connecté pourrait contenir les données spécifiques recherchées ; habiliter les autorités chargées de l'enquête à étendre la perquisition ou l'accès par un moyen similaire autorisés d'un système informatique spécifique à un autre système informatique connecté lorsqu'il existe des raisons analogues de penser que les données spécifiques recherchées sont stockées dans l'autre système informatique ; ou exercer les pouvoirs de perquisition ou d'accès similaire aux deux endroits d'une façon coordonnée et rapide.

Dans tous les cas de figure, les données à rechercher doivent être légalement accessibles à partir du système informatique initial ou disponible pour ce système initial.

195. Cet article ne traite pas des « perquisition et saisie transfrontières », qui donnent aux Etats une possibilité de perquisition ou un moyen d'accès similaire aux données se trouvant sur le territoire d'autres Etats sans avoir à recourir aux modalités habituelles de l'entraide judiciaire. On reviendra sur cette question au chapitre consacré à la coopération internationale.

196. Le paragraphe 3 aborde les questions soulevées par l'habilitation des autorités compétentes à saisir ou obtenir par un moyen similaire les données informatiques ayant fait l'objet d'une perquisition ou d'un accès par un moyen similaire en application des paragraphes 1 et 2. Les mesures prévues incluent la saisie du matériel et des supports de stockage informatiques. Dans certains cas, par exemple lorsque les données sont stockées dans un système d'exploitation dont la spécificité ne permet pas de réaliser une copie des données, il n'y a pas d'autre solution que de saisir le support de stockage lui-même. Cela peut également être nécessaire lorsque le support doit être examiné pour en extraire des données anciennes qui ont été écrasées mais qui n'en ont pas moins laissé des traces sur le support.

197. Dans le cadre de cette Convention, « saisir » veut dire emporter le support physique dans lequel les données ou les informations sont stockées ou réaliser ou conserver une copie de ces données ou informations. Ce mot implique également l'utilisation ou la saisie des programmes nécessaires pour accéder aux données à saisir. En même temps que l'utilisation du terme classique « saisir », il a été employé l'expression « obtenir par un moyen similaire » pour rendre compte des autres façons d'enlever des données intangibles, de les rendre inaccessibles ou d'en prendre le contrôle d'une autre manière dans l'environnement informatique. Etant donné que les mesures concernent des données intangibles stockées, les autorités compétentes doivent prendre des mesures supplémentaires pour obtenir les données, à savoir « préserver l'intégrité des données » ou préserver la « chaîne de garde » des données, ce qui veut dire que les données copiées ou enlevées doivent être conservées dans l'état où elles ont été trouvées au moment de la saisie et non modifiées pendant la procédure pénale. L'expression renvoie ainsi à la prise de contrôle sur les données ou à leur enlèvement.

198. Le fait de rendre des données inaccessibles peut signifier leur codage ou le blocage par tout autre moyen technique de l'accès à ces données. Cette

mesure pourrait être utilement appliquée dans des situations de danger ou de préjudice pour la société, causé par exemple par des virus ou par la présentation du mode de fabrication des virus ou des bombes, ou dans celles dans lesquelles les données ou leur contenu sont illégales, comme en cas de pornographie infantile. Le terme « enlèvement » vise à traduire l'idée que, si les données sont enlevées ou rendues inaccessibles, elles ne sont pas détruites et continuent d'exister. La personne suspecte est temporairement privée de l'accès aux données, mais celui-ci peut lui être restitué à l'issue de l'enquête ou de la procédure pénale.

199. On constate ainsi que la saisie ou l'obtention de données par un moyen similaire a deux fonctions : 1) collecter des preuves, par exemple en copiant les données, ou 2) confisquer les données, par exemple en les copiant et en rendant ultérieurement la version originelle inaccessible ou en l'enlevant. La saisie n'implique pas un effacement définitif des données saisies.

200. Le paragraphe 4 instaure une mesure coercitive destinée à faciliter la perquisition et la saisie de données informatiques. Il traite de la difficulté pratique que peuvent poser l'accès aux données recherchées et leur identification comme preuves du fait de la quantité de données pouvant être traitées et stockées, des mesures de sécurité employées et de la nature des opérations informatiques. Partant de la constatation qu'il peut y avoir lieu de consulter les administrateurs de système, qui connaissent bien le système informatique en question sur la meilleure manière de mener la perquisition, cette disposition habilite les services de lutte contre la criminalité à obliger un administrateur de système à apporter l'aide raisonnablement nécessaire pour permettre l'application d'une mesure de perquisition et de saisie.

201. Ce pouvoir ne profite pas qu'aux autorités chargées de l'enquête. Si elles ne pouvaient s'assurer cette coopération, elles pourraient rester sur les lieux de la perquisition et rendre impossible l'accès au système informatique pendant une longue période. Cela pourrait créer un fardeau économique pour des entreprises légitimes ou leurs clients et abonnés se trouvant dans l'impossibilité d'accéder aux données pendant la perquisition. En se ménageant la coopération de personnes compétentes, on peut rendre une perquisition plus efficace et moins coûteuse, tant pour les services de lutte contre la criminalité que pour les personnes innocentes touchées par cette mesure. En contraignant légalement un administrateur de système à coopérer, on peut également le décharger de toute obligation contractuelle ou autre de non-divulgaration des données.

202. Les informations que l'on peut obliger l'administrateur de système à fournir sont celles qui sont nécessaires pour permettre d'appliquer la mesure de perquisition et de saisie ou de mettre en œuvre un moyen similaire d'accès et d'obtention de données. Seules toutefois doivent être fournies les informations «raisonnablement» nécessaires. Dans certains cas, il pourra s'agir de communiquer un mot de passe ou une autre mesure de sécurité aux autorités chargées de l'enquête. Mais dans d'autres circonstances, cela ne sera pas raisonnable, comme dans le cas où la divulgation du mot de passe ou d'une autre mesure de sécurité constituerait une menace inacceptable à la vie privée d'autres utilisateurs ou au caractère confidentiel d'autres données dont la recherche n'est pas autorisée. En pareil cas, la fourniture des «informations ... nécessaires» pourrait consister à communiquer, sous une forme intelligible et lisible, les données effectivement recherchées par les autorités compétentes.

203. En vertu du paragraphe 5 de cet article, les mesures sont subordonnées aux conditions et sauvegardes prévues par le droit interne sur la base de l'article 15 de la Convention. Parmi ces conditions peuvent figurer des dispositions régissant le recrutement et la rémunération des témoins et des experts.

204. Dans le cadre du paragraphe 5, les rédacteurs ont aussi étudié la question de savoir s'il convenait de notifier aux parties intéressées le déclenchement d'une procédure de perquisition. Dans l'environnement en ligne, il peut être moins évident que des données ont fait l'objet d'une perquisition et ont été saisies (copiées) que dans l'environnement hors ligne, où les objets saisis sont physiquement absents. La législation de certaines Parties ne prévoit pas l'obligation d'indiquer une mesure de perquisition classique. En imposant la notification d'une perquisition informatique, la Convention introduirait une anomalie dans la législation de ces Parties. D'un autre côté, certains Etats pourraient voir dans la notification un élément essentiel de la mesure, qui permettrait d'établir une distinction entre la recherche de données informatiques stockées dans le cadre d'une perquisition (qui n'est généralement pas conçue comme une mesure subreptice) et l'interception de données en cours de transmission (qui est une mesure subreptice, voir les articles 20 et 21). La question de la notification est donc laissée à l'appréciation du droit interne. Si les Parties envisagent d'établir un système de notification obligatoire aux personnes concernées, il convient de ne pas perdre de vue que cette notification risque de nuire au bon déroulement de l'enquête. En présence d'un tel risque, il conviendrait d'envisager l'ajournement de la notification.

Titre 5 – Collecte en temps réel de données informatiques

205. Les articles 20 et 21 prévoient la collecte en temps réel de données relatives au trafic et l'interception en temps réel de données relatives au contenu associées à des communications précises transmises au moyen d'un système informatique. Ces dispositions traitent de la collecte et de l'interception en temps réel de ces données par des autorités compétentes, ainsi que de leur collecte ou interception par des fournisseurs de services. Elles abordent également l'obligation de confidentialité.

206. L'interception de télécommunications concerne habituellement les réseaux de télécommunications classiques. Ces réseaux peuvent comprendre des infrastructures câblées (câbles métalliques ou à fibres optiques), ainsi que des interconnexions avec des réseaux sans fil, dont les systèmes de téléphonie mobile et les systèmes de transmission par micro-ondes. Aujourd'hui, les communications mobiles sont facilitées par un système de réseaux satellitaires spécialisés. Les réseaux informatiques peuvent également consister en une infrastructure câblée fixe indépendante, mais il arrive plus souvent qu'ils soient exploités sous la forme d'un réseau virtuel à l'aide de connexions réalisées par le biais d'infrastructures de télécommunications, ce qui permet de créer des réseaux informatiques ou des réseaux de réseaux d'ampleur mondiale. La convergence des technologies des télécommunications et de l'information brouille les distinctions entre télécommunications et téléinformatique et les spécificités de leurs infrastructures. Ainsi la définition du « système informatique » donnée à l'article 1 ne limite-t-elle pas la manière dont les dispositifs ou groupes de dispositifs peuvent être interconnectés. Il s'ensuit que les articles 20 et 21 s'appliquent à des communications spécifiées transmises au moyen d'un système informatique, la communication pouvant être transmise par le biais d'un réseau de télécommunications avant d'être reçue par un autre système informatique.

207. Les articles 20 et 21 n'établissent pas de distinction entre un système de télécommunications ou informatique public et privé ou, en ce qui concerne l'utilisation des systèmes et des services de communication, entre les utilisateurs publics et les groupes fermés d'utilisateurs et correspondants privés. La définition du « fournisseur de services » donnée à l'article 1 se rapporte aux entités publiques et privées qui offrent aux usagers de leurs services la possibilité de communiquer au moyen d'un système informatique.

208. Ce titre est applicable à la collecte de preuves contenues dans des communications en cours de production et collectées au moment de la transmission de la communication (c'est-à-dire « en temps réel »). Les données

se présentent sous une forme intangible (par exemple sous la forme de transmissions d'impulsions vocales ou électroniques). La collecte ne perturbe pas sensiblement la circulation des données et la communication atteint son destinataire. Au lieu de procéder à une saisie physique des données, on fait un enregistrement (c'est-à-dire une copie) des données en cours de transmission. La collecte de ces informations est effectuée pendant une période donnée. Un mandat est demandé pour autoriser la collecte de données se rapportant à un événement futur (c'est-à-dire une future transmission de données).

209. Les données pouvant être collectées sont de deux types : les données relatives au trafic et les données relatives au contenu. Au sens de l'article 1, les « données relatives au trafic » désignent toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, avec indication des informations suivantes : origine, destination, itinéraire, heure, date, taille et durée de la communication ou type de service. Les « données relatives au contenu » ne sont pas définies dans la Convention, mais désignent le contenu informatif de la communication, c'est-à-dire le sens de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic).

210. De nombreux Etats établissent une distinction entre l'interception en temps réel de données relatives au contenu et la collecte en temps réel de données relatives au trafic du double point de vue des conditions juridiques devant être préalablement réunies pour autoriser une telle mesure d'enquête et des infractions au titre desquelles on peut recourir à cette mesure. Tout en admettant que les deux types de données peuvent mettre en jeu des intérêts de nature privée, beaucoup d'Etats considèrent, que dans le cas des données relatives au contenu, ces intérêts sont supérieurs du fait même de la nature du contenu ou du message de la communication. La collecte de données relatives au contenu peut donc faire l'objet de restrictions plus importantes que dans le cas des données relatives au trafic. Pour aider à apprécier cette distinction, la Convention, tout en constatant sur le plan opérationnel que les données sont collectées ou enregistrées dans les deux situations, désigne sur le plan normatif, dans les titres des articles, la collecte des données relatives au trafic sous l'appellation de « collecte en temps réel » et la collecte des données relatives au contenu sous l'appellation d'« interception en temps réel ».

211. Dans certains Etats, la législation en vigueur ne fait aucune distinction entre la collecte de données relatives au trafic et l'interception de données

relatives au contenu, soit parce qu'aucune distinction n'a été inscrite dans la loi en ce qui concerne les différences sur le plan des intérêts de nature privée, soit parce que les techniques de collecte concernant les deux mesures se ressemblent beaucoup. Ainsi les conditions juridiques à remplir pour autoriser l'application des mesures et les infractions au titre desquelles il peut être recouru à ces mesures sont-elles identiques. La Convention constate cette situation en faisant le même usage opérationnel de l'expression «collecter ou enregistrer» dans le libellé des deux articles 20 et 21.

212. S'agissant de l'interception en temps réel des données relatives au contenu, la loi prévoit souvent que l'on ne peut recourir à cette mesure que dans le cadre d'une enquête ouverte sur une infraction grave ou une catégorie d'infractions graves. Le droit interne identifie souvent les infractions en question comme étant graves à ce titre en les faisant figurer dans une liste d'infractions à laquelle la mesure peut être appliquée ou en les faisant relever de cette catégorie en se référant à une certaine peine d'emprisonnement maximale dont l'infraction est punissable. Aussi, en ce qui concerne l'interception des données relatives au contenu, l'article 21 dispose expressément que les Parties ne sont tenues d'instaurer cette mesure qu'«en relation avec de graves infractions à définir dans le droit interne».

213. En revanche, l'article 20, qui se rapporte à la collecte des données relatives au trafic, n'est pas assorti des mêmes limitations et s'applique en principe à toute infraction pénale visée par la Convention. Toutefois, le paragraphe 3 de l'article 14 dispose qu'une Partie peut se réserver le droit de n'appliquer cette mesure qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique la mesure d'interception des données relatives au contenu. Néanmoins, la Partie qui fait pareille réserve doit envisager de la limiter de manière à permettre l'application la plus large possible de la mesure de collecte des données relatives au trafic.

214. Pour certains Etats, les infractions créées dans la Convention ne sont normalement pas considérées comme suffisamment graves pour donner lieu à l'interception des données relatives au contenu voire, dans certains cas, à la collecte des données relatives au trafic. Quoi qu'il en soit, ces techniques sont souvent essentielles pour l'enquête ouverte sur certaines des infractions créées dans la Convention, telles que celles qui impliquent un accès illicite aux systèmes informatiques, la diffusion de virus ou la pornographie infantile. Il arrive, par exemple, que la source de l'intrusion ou de

la diffusion ne puisse pas être établie sans que l'on ait recours à la collecte en temps réel de données relatives au trafic. Dans certains cas, la nature de la communication ne peut être découverte sans interception en temps réel des données relatives au contenu. Ces infractions, par leur nature ou le mode de transmission utilisé, impliquent l'utilisation de technologies informatiques. La mise en œuvre de moyens technologiques devrait donc être autorisée pour enquêter sur ces infractions. Toutefois, la question de l'interception des données relatives au trafic pouvant soulever des problèmes délicats, la Convention laisse la portée de cette mesure à l'appréciation du droit interne. Certains pays assimilant juridiquement la collecte de données relatives au trafic à l'interception des données relatives au contenu, une possibilité de réserve est autorisée pour restreindre l'applicabilité de la première mesure, mais cette applicabilité ne doit pas être réduite davantage que la mesure dans laquelle une Partie restreint l'interception en temps réel des données relatives au contenu. Néanmoins, les Parties devraient envisager d'appliquer les deux mesures aux infractions créées dans la Convention (section 1, chapitre II) afin d'offrir un moyen efficace aux autorités chargées d'enquêter sur ces infractions informatiques et infractions en relation avec l'ordinateur.

215. Les conditions et sauvegardes touchant les pouvoirs et procédures se rapportant à l'interception en temps réel des données relatives au contenu et à la collecte en temps réel des données relatives au trafic sont subordonnées aux articles 14 et 15. Etant donné que l'interception des données relatives au contenu est une mesure très intrusive sur le plan de la vie privée, il est nécessaire de mettre en place des mesures rigoureuses de sauvegarde pour garantir un équilibre approprié entre les intérêts de la justice et les droits fondamentaux de la personne humaine. Dans le domaine de l'interception, la présente Convention n'énonce pas de sauvegardes spécifiques si ce n'est qu'elle limite l'autorisation de l'interception des données relatives au contenu aux enquêtes ouvertes sur des infractions pénales graves définies dans le droit interne. Néanmoins, les conditions et sauvegardes importantes dans ce domaine, appliquées dans la législation nationale, sont les suivantes : supervision judiciaire ou autre mode de supervision indépendante ; nécessité de désigner expressément les communications à intercepter ou les personnes concernées ; nécessité, subsidiairement et proportionnalité (par exemple les conditions juridiques justifiant l'application de la mesure ; l'inefficacité d'autres mesures moins intrusives) ; limitation de la durée de l'interception ; droit de recours. Beaucoup de ces sauvegardes se situent dans la ligne de la Convention européenne des droits de l'homme et de sa jurisprudence ultérieure (voir les arrêts rendus dans les

affaires *Klass*⁵, *Kruslin*⁶, *Huvig*⁷, *Malone*⁸, *Halford*⁹ et *Lambert*¹⁰). Certaines de ces sauvegardes sont également applicables à la collecte en temps réel des données relatives au trafic.

Collecte en temps réel des données relatives au trafic (article 20)

216. Souvent, les données relatives au trafic initiales peuvent ne plus être disponibles ou n'être plus utilisables parce que l'intrus a modifié le chemin de la communication. Il s'ensuit que la collecte en temps réel de données relatives au trafic est une importante mesure d'enquête. L'article 20 traite de la question de la collecte et de l'enregistrement en temps réel des données relatives au trafic aux fins d'enquêtes ou de procédures pénales spécifiques.

217. La collecte des données relatives au trafic concernant les télécommunications (par exemple les conversations téléphoniques) a toujours été un instrument d'enquête utile pour établir la source ou la destination (par exemple les numéros de téléphone) et des données connexes (comme l'heure, la date et la durée) concernant différents types de communications illégales (par exemple les menaces et actes d'intimidation criminels, les complots criminels et les allégations frauduleuses) et de communications donnant des preuves d'infractions passées ou futures (par exemple trafic de stupéfiants, meurtre et délits économiques).

218. Les communications informatiques peuvent constituer ou prouver les mêmes types d'actes criminels. Toutefois, comme la technologie informatique est capable de transmettre de grandes quantités de données – texte, images et sons –, elle offre de plus vastes possibilités de commettre des infractions mettant en jeu la diffusion de contenu illégal (par exemple de la pornographie infantine). De même, comme les ordinateurs peuvent stocker de grandes quantités de données, qui ont souvent un caractère privé, le risque de causer un préjudice – économique, social ou personnel – peut être important si l'intégrité de ces données est compromise. En outre, comme la science informatique repose sur le traitement de données, que celles-ci soient un produit final ou qu'elles soient un élément d'une fonction opérationnelle (comme l'exécution de programmes informatiques), toute ingérence dans ces données peut avoir

5. Arrêt rendu par la CEDH dans l'affaire *Klass et autres c. Allemagne*, A28, 06/09/1978.

6. Arrêt rendu par la CEDH dans l'affaire *Kruslin c. France*, 176-A, 24/04/1990.

7. Arrêt rendu par la CEDH dans l'affaire *Huvig c. France*, 176-B, 24/04/1990.

8. Arrêt rendu par la CEDH dans l'affaire *Malone c. Royaume-Uni*, A82, 02/08/1984.

9. Arrêt rendu par la CEDH dans l'affaire *Halford c. Royaume-Uni*, Rapports 1997 III, 25/06/1997.

10. Arrêt rendu par la CEDH dans l'affaire *Lambert c. France*, Rapports 1998 V, 24/08/1998.

des conséquences désastreuses sur le bon fonctionnement des systèmes informatiques. En cas de diffusion illicite de pornographie infantine, d'accès illégal à un système informatique, d'entrave au bon fonctionnement du système informatique ou d'atteinte à l'intégrité des données, il est absolument indispensable, surtout si l'infraction est commise à distance, par exemple par le biais de l'Internet, de reconstituer le chemin suivi par les communications entre la victime et l'auteur de l'infraction. On constate ainsi que la capacité de collecter des données relatives au trafic concernant les communications informatiques est tout aussi importante, sinon plus importante, qu'en ce qui concerne les télécommunications classiques. Cette technique d'enquête permet d'effectuer des rapprochements entre l'heure, la date et la source et la destination des communications du suspect et l'heure des intrusions dans les systèmes des victimes, d'identifier d'autres victimes ou d'établir des liens avec des complices.

219. En vertu de cet article, les données relatives au trafic doivent être associées à des communications spécifiques transmises sur le territoire de la Partie concernée. On parle de « communications » précises au pluriel car il peut s'avérer nécessaire de collecter des données relatives au trafic concernant plusieurs communications pour établir la source ou la destination humaines (par exemple dans une famille où plusieurs personnes utilisent les mêmes moyens de télécommunications, il peut être nécessaire d'établir une corrélation entre plusieurs communications et la possibilité pour chaque personne d'utiliser le système informatique). Toutefois, les communications au titre desquelles les données relatives au trafic peuvent être collectées ou enregistrées doivent être spécifiées. Il s'ensuit que la Convention ne requiert ni n'autorise la surveillance et la collecte générales ou systématiques de quantités importantes de données relatives au trafic. Elle n'autorise pas non plus les « missions exploratoires » à la faveur desquelles on espère découvrir des activités criminelles, situation très différente des enquêtes ouvertes sur des cas précis d'agissements illégitimes. L'ordonnance judiciaire ou autre autorisant la collecte doit préciser les communications auxquelles se rapporte la collecte des données relatives au trafic en question.

220. Sans préjudice du paragraphe 2, les Parties sont tenues, en application du paragraphe 1.a), de veiller à ce que leurs autorités compétentes aient la capacité de collecter ou d'enregistrer des données relatives au trafic par l'application de moyens techniques. L'article ne précise les moyens technologiques à mettre en œuvre pour procéder à cette collecte et ne définit aucune obligation en termes techniques.

221. En outre, en application du paragraphe 1.b), les Parties sont tenues de veiller à ce que leurs autorités compétentes soient habilitées à obliger un fournisseur de services à collecter ou enregistrer des données relatives au trafic ou à leur prêter coopération et assistance pour la collecte ou l'enregistrement de ces données. Cette obligation imposée aux fournisseurs de services n'est applicable que dans la mesure où la collecte ou l'enregistrement, ou la coopération et l'assistance, reste dans le cadre des capacités techniques existantes du fournisseur de services. L'article n'oblige pas les fournisseurs de services à garantir qu'ils ont les capacités techniques de procéder à la collecte ou à l'enregistrement ou de prêter coopération et assistance. Il ne leur impose pas d'acquérir ou de mettre au point de nouveaux équipements, d'engager un expert chargé de les aider, ou de procéder à une reconfiguration onéreuse de leurs systèmes. Toutefois, si leurs systèmes et leur personnel ont actuellement les capacités techniques nécessaires pour procéder à cette collecte ou à cet enregistrement ou prêter coopération et assistance à cette fin, l'article les oblige à prendre les mesures nécessaires pour mettre en œuvre ces capacités. Ainsi, par exemple, il se pourrait que le système soit configuré d'une manière qui permettrait de prendre ces mesures ou que le fournisseur de services ait déjà en sa possession les programmes informatiques lui permettant de le faire, mais que ces mesures ne soient pas habituellement appliquées ni ces programmes utilisés dans le cadre des activités normales du fournisseur de services. En pareil cas, l'article imposerait à ce dernier de mettre en œuvre ou sous tension ces dispositifs, en application des dispositions légales.

222. Comme il s'agit d'une mesure à appliquer au niveau national, les mesures sont appliquées à la collecte ou à l'enregistrement de communications précises transmises sur le territoire de la Partie concernée. Ainsi, dans la pratique, les obligations sont-elles généralement applicables lorsque le fournisseur de service dispose de certaines infrastructures ou de certains équipements sur ce territoire capables d'appliquer les mesures en question, même si ces infrastructures ou équipements se trouvent implantés dans un endroit autre que celui où il exerce son activité principale ou a son siège social. Aux fins de la Convention, une communication est réputée transmise sur le territoire d'une Partie si l'un des deux correspondants (qui sont des êtres humains ou des ordinateurs) se trouve sur ce territoire ou si le matériel informatique ou de télécommunication par le biais duquel la communication est transmise se trouve sur ce territoire.

223. D'une façon générale, les deux possibilités existantes de collecte des données relatives au trafic visées aux alinéas a) et b) du paragraphe 1 ne

sont pas alternatives. A l'exception des dispositions du paragraphe 2, une Partie doit veiller à ce que les deux mesures soient appliquées. C'est indispensable car, si un fournisseur de services n'a pas les capacités techniques de procéder à la collecte ou à l'enregistrement des données relatives au trafic [1.b)], les autorités chargées de l'application de la loi de la Partie en question doivent alors avoir la possibilité de s'en charger elles-mêmes [1.a)]. De même, l'obligation visée au paragraphe 1. b) ii) selon laquelle le fournisseur de services doit prêter aux autorités compétentes coopération et assistance pour la collecte ou l'enregistrement des données relatives au trafic n'aurait aucun sens si ces autorités n'étaient pas habilitées à collecter ou enregistrer elles-mêmes les données en question. De plus, dans le cas de certains réseaux locaux dans lequel il se peut qu'aucun fournisseur de services ne soit concerné, la seule façon de réaliser la collecte ou l'enregistrement des données consisterait pour les autorités chargées de l'enquête à y procéder elles-mêmes. Les deux mesures prévues aux alinéas a) et b) du paragraphe 1 n'ont pas à être appliquées dans tous les cas, mais l'article exige que les deux méthodes soient disponibles.

224. Toutefois, cette double obligation a créé des difficultés pour certains Etats dans lesquels les autorités chargées de l'application de la loi ne peuvent intercepter des données dans des systèmes de télécommunications qu'avec le concours d'un fournisseur de services ou ne peuvent le faire de façon subreptice, sans qu'au moins le fournisseur de services en ait connaissance. Une telle situation est prise en considération au paragraphe 2. Lorsqu'une Partie, en raison des « principes établis de son ordre juridique interne », ne peut adopter les mesures énoncées au paragraphe 1.a), elle peut, au lieu de celles-ci, adopter une approche différente, consistant par exemple à n'obliger les fournisseurs de services qu'à fournir les équipements techniques nécessaires pour que les autorités chargées de l'application de la loi puisse collecter en temps réel les données relatives au trafic. En pareil cas, toutes les autres limitations concernant le territoire, la spécificité des communications et la mise en œuvre des moyens techniques restent applicables.

225. Comme l'interception en temps réel des données relatives au contenu, la collecte en temps réel des données relatives au trafic n'est efficace que si elle est effectuée à l'insu des personnes faisant l'objet d'une enquête. Subreptice par nature, l'interception doit être effectuée d'une manière telle que les correspondants n'aient pas conscience de l'opération. Les fournisseurs de services et leurs employés qui sont au courant doivent donc être tenus de garder le secret pour que la procédure puisse être efficace.

226. Le paragraphe 3 fait obligation aux Parties d'adopter les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder la confidentialité quant au fait que l'une ou l'autre des mesures prévues dans le présent article concernant la collecte en temps réel des données relatives au trafic a été appliquée ainsi que toute information à ce sujet. Cette disposition non seulement garantit la confidentialité de l'enquête, mais décharge le fournisseur de services de toute obligation contractuelle ou de toute autre obligation juridique d'aviser ses abonnés que des données les concernant sont collectées. La mise en œuvre du paragraphe 3 peut donner lieu à l'instauration d'obligations explicites en droit interne. D'un autre côté, une Partie peut être en mesure d'assurer la confidentialité de la mesure en se fondant sur d'autres dispositions du droit interne, telles que le pouvoir de poursuivre pour entrave à la bonne marche de la justice les personnes qui aident les délinquants en les informant de la mesure dont ils font l'objet. Il est préférable d'instaurer une règle de confidentialité (assortie d'une sanction effective en cas de violation), mais il est aussi possible de recourir aux entraves à la bonne marche de la justice pour prévenir toute divulgation intempestive, ce qui est suffisant pour la mise en œuvre de ce paragraphe. Lorsque des obligations expresses de confidentialité sont créées, elles doivent être subordonnées aux conditions et sauvegardes prévues aux articles 14 et 15. Vu la nature subreptice de la mesure d'enquête, ces sauvegardes ou conditions devraient fixer une durée maximale raisonnable pour l'obligation.

227. Comme on l'a vu plus haut, on considère généralement que l'intérêt de nature privée est moindre en ce qui concerne la collecte des données relatives au trafic que dans le cas de l'interception des données relatives au contenu. En effet, les données relatives au trafic concernant l'heure, la durée ou la taille de la communication ne révèlent guère d'informations de caractère personnel sur un individu ou sa façon de penser. En revanche, les données concernant la source ou la destination d'une communication (par exemple les sites Web visités) peuvent soulever des questions plus délicates au regard du droit au respect de la vie privée. La collecte de ces données peut, dans certaines situations, permettre d'établir une description des intérêts de la personne concernée, des personnes qui lui sont associées et du cadre social dans lequel elle évolue. Les Parties devraient en tenir compte au moment d'instaurer les sauvegardes appropriées et les conditions juridiques préalables à l'application de ces mesures, conformément aux articles 14 et 15.

Interception de données relatives au contenu (article 21)

228. La collecte de données relatives au contenu des télécommunications (comme les conversations téléphoniques) a toujours été un instrument d'enquête utile pour déterminer si la communication a un caractère illégal (par exemple, une menace ou un acte d'intimidation criminel, un complot criminel ou des allégations frauduleuses) et apporter la preuve d'infractions passées ou futures (comme le trafic de stupéfiants, le meurtre ou les délits économiques). Les communications informatiques peuvent constituer ou prouver les mêmes types d'actes criminels. Toutefois, comme la technologie informatique est capable de transmettre de grandes quantités de données – texte, images et sons –, elle offre de plus vastes possibilités de commettre des infractions mettant en jeu la diffusion de contenu illégal (par exemple de la pornographie infantine). La commission de nombreuses infractions informatiques suppose la transmission ou la communication de données ; c'est le cas des communications envoyées pour accéder de façon illicite à un système informatique ou de la diffusion de virus informatiques. Il n'est pas possible de déterminer en temps réel la nature préjudiciable et illégale de ces communications sans intercepter le contenu du message. Si elles ne pouvaient pas établir et prévenir la commission d'infractions au moment où elles ont eu lieu, les autorités chargées de l'application de la loi en seraient réduites à enquêter sur des infractions révolues, dans le cas desquelles le préjudice a déjà été causé. On voit que l'interception en temps réel des données relatives au contenu des communications informatiques est au moins, sinon plus importante que l'interception en temps réel des télécommunications.

229. Par « données relatives au contenu », il faut entendre le contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic.

230. La plupart des éléments de cet article sont identiques à ceux de l'article 20. En conséquence, les commentaires ci-dessus concernant la collecte ou l'enregistrement des données relatives au trafic, l'obligation de prêter coopération et assistance et l'obligation de confidentialité s'appliquent de la même façon à l'interception des données relatives au contenu. Etant donné que les données relatives au contenu soulèvent davantage de questions au regard du droit au respect de la vie privée, la mesure d'enquête est limitée à « de graves infractions à définir dans le droit interne ».

231. De même, comme indiqué dans les commentaires ci-dessus concernant l'article 20, les conditions et sauvegardes applicables à l'interception en temps réel des données relatives au contenu peuvent être plus rigoureuses que celles qui s'appliquent à la collecte en temps réel des données relatives au trafic ou à la perquisition et à la saisie, ainsi qu'à tout autre moyen d'accès et d'obtention des données stockées.

Section 3 – Compétence

Compétence (article 22)

232. Cet article établit une série de critères en vertu desquels les Parties contractantes sont tenues d'établir leur compétence relativement aux infractions pénales visées aux articles 2 à 11 de la Convention.

233. Le paragraphe 1 *lettre a* s'appuie sur le principe de territorialité. Chaque Partie est tenue de punir la commission d'infractions établies dans la Convention lorsqu'elles sont commises sur son territoire. Ainsi, par exemple, une Partie pourrait revendiquer une compétence territoriale dans le cas où la personne responsable de l'attaque commise contre un système informatique et le système victime de l'attaque se trouvent tous deux sur son territoire, et dans celui où le système informatique attaqué se trouve sur son territoire, même si l'auteur de l'attaque ne s'y trouve pas.

234. La possibilité d'inclure une disposition obligeant chaque Partie à établir sa compétence relativement à des infractions impliquant des satellites immatriculés dans cette Partie a été examinée. Les auteurs ont décidé qu'une telle disposition était inutile car les communications illicites impliquant des satellites ne pouvaient provenir que de la Terre et/ou être reçues sur la Terre. L'un des fondements de la compétence d'une Partie énoncés au paragraphe 1 *lettre a à c* s'appliquerait si la transmission provient de l'un des lieux qui y sont cités ou y aboutit. De plus, dans la mesure où l'infraction impliquant une communication par satellite est commise par un ressortissant de l'une des Parties sans relever de la compétence territoriale d'un quelconque Etat, le paragraphe 1 *lettre d* établit une compétence. Enfin, les auteurs se sont demandé si l'immatriculation était un fondement approprié pour établir une compétence pénale dans la mesure où, bien souvent, il n'existe pas de lien véritable entre l'infraction commise et l'Etat d'immatriculation puisque un satellite n'est qu'un simple moyen de transmission.

235. Les *lettres b et c* du paragraphe 1 s'appuient sur une variante du principe de territorialité. Ces dispositions imposent à chaque Partie d'établir sa

compétence relativement à des infractions commises à bord de navires battant son pavillon ou d'aéronefs immatriculés dans cette Partie. Cette obligation est déjà en vigueur dans la législation de nombreux Etats car ces navires et aéronefs sont souvent considérés comme une extension du territoire de l'Etat. Ce type de compétence est très utile lorsque le navire ou l'aéronef ne se trouvent pas sur le territoire de la Partie au moment où l'infraction est commise, le paragraphe 1 *lettre a* ne pouvant alors servir à établir la compétence. Si l'infraction est commise à bord d'un navire ou d'un aéronef se trouvant en dehors du territoire de l'Etat du pavillon ou d'immatriculation, il se pourrait qu'aucun autre Etat ne puisse exercer sa compétence si cette règle n'existait pas. En outre, si une infraction est commise à bord d'un navire ou d'un aéronef qui ne fait qu'emprunter les eaux ou l'espace aérien d'un autre Etat, ce dernier Etat peut rencontrer des obstacles concrets importants à l'exercice de sa compétence ; il est alors utile que l'Etat d'immatriculation puisse également exercer sa compétence.

236. Le paragraphe 1, *lettre d* s'appuie sur le principe de nationalité. La théorie de la nationalité est le plus souvent invoquée par les Etats de tradition civiliste. Elle dispose que les ressortissants d'un Etat sont tenus de se conformer au droit interne même lorsqu'ils se trouvent en dehors de son territoire. En vertu de la *lettre d*, si un ressortissant commet une infraction à l'étranger, la Partie est tenue d'avoir la possibilité d'engager les poursuites correspondantes si l'infraction est également punissable en vertu du droit de l'Etat dans lequel elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

237. Le paragraphe 2 permet aux Parties de formuler une réserve à l'égard des règles de compétence définies au paragraphe 1, *lettres b, c et d*. Toutefois, aucune réserve n'est autorisée en ce qui concerne l'établissement de la compétence territoriale visée à la *lettre a* ou l'obligation d'établir la compétence dans les affaires relevant du principe « *aut dedere aut judicare* » (extrader ou poursuivre) visé au paragraphe 3, c'est-à-dire lorsque cette Partie a refusé d'extrader l'auteur présumé de l'infraction au titre de sa nationalité et que celui-ci est présent sur son territoire. La compétence établie en vertu du paragraphe 3 est nécessaire pour garantir que la Partie qui refuse d'extrader un ressortissant ait la possibilité juridique d'ouvrir une enquête et d'engager des poursuites sur son territoire, si la Partie ayant sollicité l'extradition conformément aux dispositions du paragraphe 6 de l'article 24, « Extradition », de la Convention le lui demande.

238. Les règles de compétence énoncées au paragraphe 1 ne sont pas exclusives. Le paragraphe 4 de cet article autorise les parties à établir, conformément à leur droit interne, d'autres types de compétence pénale.

239. Dans le cas d'infractions commises au moyen de systèmes informatiques, il peut arriver que plusieurs Parties aient compétence à l'égard de certaines ou de toutes les personnes ayant participé à la commission d'une infraction donnée. Ainsi, par exemple, un grand nombre d'attaques par des virus, d'escroqueries et d'atteintes à la propriété intellectuelle commises par le moyen de l'Internet ont pour cibles des victimes se trouvant dans de nombreux Etats. Afin d'éviter tout chevauchement d'activités, tout désagrément inutile aux témoins, toute concurrence entre les services de répression des Etats concernés ou afin de renforcer à d'autres égards l'efficacité ou l'équité des procédures, les Parties concernées doivent se consulter afin de décider quelle est la juridiction la mieux à même d'exercer les poursuites. Dans certains cas, les Etats ont tout intérêt, pour des raisons d'efficacité, à choisir un lieu de poursuite unique ; dans d'autres, le mieux est qu'un Etat poursuive certains participants, tandis qu'un autre Etat ou plusieurs autres Etats poursuivent d'autres participants. Ce paragraphe permet de recourir à l'une ou l'autre solution. Enfin, l'obligation de consultation n'est pas absolue, mais la consultation doit avoir lieu « lorsque cela est opportun. » Ainsi, par exemple, si l'une des Parties sait que la consultation n'est pas nécessaire (par exemple lorsqu'elle a reçu confirmation que l'autre partie n'envisage pas d'engager des poursuites), ou qu'une partie estime que la consultation pourrait nuire à l'enquête qu'elle a ouverte ou à la procédure qu'elle a engagée, elle peut repousser ou refuser cette consultation.

Chapitre III – Coopération internationale

240. Le chapitre III contient un certain nombre de dispositions relatives à l'extradition et à l'entraide judiciaire entre les Parties.

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Principes généraux relatifs à la coopération internationale (article 23)

241. L'article 23 énonce trois principes généraux devant régir la coopération internationale prévue au chapitre III.

242. En premier lieu, l'article précise que les Parties doivent coopérer les unes avec les autres « dans la mesure la plus large possible. » Ce principe fait

obligation aux Parties de coopérer largement les unes avec les autres et de réduire autant que faire se peut les obstacles à la circulation rapide et sans problème, au plan international, de l'information et des preuves.

243. Ensuite, l'article 23 énonce la portée générale de l'obligation de coopérer : la coopération doit s'étendre à toutes les infractions pénales liées à des systèmes et données informatiques (c'est-à-dire les infractions visées par l'article 14, paragraphe 2, *lettres a et b*), ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. En d'autres termes, les clauses du chapitre III sont applicables soit aux situations où l'infraction est commise à l'aide d'un système informatique, soit à celles où une infraction ordinaire, non commise à l'aide d'un système informatique (par exemple un meurtre), donne lieu à la collecte de preuves sous forme électronique. Toutefois, il convient de noter que les articles 24 (extradition), 33 (entraide dans la collecte en temps réel de données relatives au trafic) et 34 (entraide en matière d'interception de données relatives au contenu) autorisent les Parties à modifier le champ d'application de ces mesures.

244. Enfin, cette coopération doit être mise en œuvre à la fois « conformément aux dispositions du présent chapitre » et « en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements établis sur la base des législations uniformes ou réciproques et [du] droit national. » Cette dernière clause établit le principe général suivant lequel les dispositions du chapitre III n'annulent ni ne remplacent les dispositions des instruments internationaux sur l'entraide judiciaire et l'extradition, les arrangements réciproques entre les Parties à ces instruments (sur lesquels on reviendra en détail dans l'analyse de l'article 27 ci-après) ou les dispositions pertinentes du droit national relatives à la coopération internationale. Ce principe de base est expressément renforcé dans les articles 24 (extradition), 25 (principes généraux relatifs à l'entraide), 26 (information spontanée), 27 (procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables), 28 (confidentialité et restriction d'utilisation), 31 (entraide concernant l'accès aux données stockées), 33 (entraide dans la collecte en temps réel de données relatives au trafic) et 34 (entraide en matière d'interception de données relatives au contenu).

Titre 2 – Principes relatifs à l'extradition

Extradition (article 24)

245. Le paragraphe 1 précise que l'obligation d'extrader ne s'applique qu'aux infractions définies conformément aux articles 2 à 11 de la Convention qui

sont punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an ou par une peine plus sévère. Les auteurs ont décidé de prévoir une peine minimale car, en vertu de la Convention, les Parties peuvent punir certaines des infractions d'une peine maximale d'emprisonnement relativement courte (comme dans le cas de l'article 2 – accès illégal – et de l'article 4 – atteinte à l'intégrité des données). Les auteurs n'ont donc pas jugé bon de requérir que chacune des infractions établies aux articles 2 à 11 soit considérée *ipso facto* comme pouvant donner lieu à extradition. En conséquence, ils se sont entendus sur une disposition suivant laquelle une infraction doit être considérée comme pouvant donner lieu à extradition si – comme indiqué dans l'article 2 de la Convention européenne d'extradition (STE n° 24) – la peine maximale pouvant être imposée dans le cas d'une infraction dont l'auteur faisait l'objet d'une demande d'extradition était d'au moins un an d'emprisonnement. La question de savoir si une infraction peut ou non donner lieu à extradition n'est pas liée à la peine effectivement imposée dans chaque cas d'espèce, mais plutôt à la période maximale pouvant légalement être imposée dans le cas de l'infraction pour laquelle l'extradition est demandée.

246. D'un autre côté, en application du principe général selon lequel la coopération internationale prévue au chapitre III doit être mise en œuvre conformément aux dispositions des instruments en vigueur entre les Parties, le paragraphe 1 prévoit également que lorsqu'un traité d'extradition ou un arrangement établi sur la base des législations uniformes ou réciproques est en vigueur entre deux ou plusieurs Parties (voir l'analyse de cette expression dans le passage consacré à l'article 27 ci-après) et que ce texte prévoit, pour qu'il y ait extradition, une peine minimale différente, c'est la peine minimale prévue par le traité ou l'arrangement en question qui s'applique. Ainsi, par exemple, de nombreux traités d'extradition passés entre des pays européens et des pays non européens prévoient qu'une infraction ne peut donner lieu à extradition que si la peine maximale est une peine d'emprisonnement d'une durée *supérieure* à un an ou que la peine est plus sévère. En pareil cas, les spécialistes de l'extradition continueront d'appliquer la peine minimale normalement prévue par leur pratique conventionnelle afin de déterminer si une infraction peut donner lieu à extradition. Même en vertu de la Convention européenne d'extradition (STE n° 24), les réserves peuvent prévoir une peine minimale différente pour l'extradition. Dans les situations impliquant des Parties à cette Convention, lorsqu'une Partie ayant formulé une telle réserve reçoit une demande d'extradition, il convient de se fonder sur la peine prévue dans la réserve pour déterminer si l'infraction peut donner lieu à extradition.

247. Le paragraphe 2 dispose que les infractions décrites au paragraphe 1 doivent être considérées comme des infractions pouvant donner lieu à extradition dans tout traité d'extradition existant ou pouvant être conclu entre les Parties et doivent être incluses dans les traités qu'elles pourraient négocier entre elles à l'avenir. Cela ne veut pas dire que l'extradition doive être accordée chaque fois qu'une demande en ce sens est présentée, mais plutôt que la possibilité de faire droit à une demande d'extradition visant des personnes ayant commis ce type d'infraction doit exister. En vertu du paragraphe 5, les Parties peuvent soumettre l'extradition à d'autres conditions.

248. En application du paragraphe 3, une Partie qui n'accorderait pas l'extradition, soit parce qu'elle n'a pas conclu de traité d'extradition avec la Partie requérante, soit parce que le traité existant ne permet pas de faire droit à une demande présentée au titre de l'une des infractions établies conformément à cette Convention, peut considérer celle-ci comme fondement juridique pour remettre la personne dont l'extradition est demandée, bien qu'elle n'y soit pas tenue.

249. Lorsqu'une Partie, au lieu de s'en remettre à un traité d'extradition, se prévaut d'un texte réglementaire général pour procéder à l'extradition, elle est tenue, conformément au paragraphe 4, d'inclure les infractions mentionnées au paragraphe 1 parmi celles au regard desquelles l'extradition est possible.

250. Le paragraphe 5 prévoit que la Partie requise n'est pas tenue d'extrader si elle estime que les conditions prévues par le traité en vigueur ou le droit interne ne sont pas remplies. C'est un autre exemple du principe selon lequel la coopération doit être mise en œuvre conformément aux dispositions des instruments internationaux en vigueur entre les Parties, des arrangements établis sur la base des législations uniformes ou réciproques ou du droit national. Ainsi, par exemple, les conditions et restrictions énoncées dans la Convention européenne d'extradition (STE n° 24) et ses Protocoles additionnels (STE n°s 86 et 98) s'appliquent aux Parties à ces instruments, lesquelles peuvent refuser l'extradition sur cette base (par exemple, l'article 3 de la Convention européenne d'extradition prévoit que l'extradition ne sera pas accordée si l'infraction est considérée comme une infraction politique ou si la demande est réputée avoir été faite aux fins de poursuivre ou de punir une personne pour des raisons tenant, entre autres, à sa race, à sa religion, à sa nationalité ou à ses opinions politiques).

251. Le paragraphe 6 applique le principe « *aut dedere aut judicare* » (extrader ou poursuivre). Etant donné que beaucoup d'Etats refusent d'extrader leurs ressortissants, les auteurs d'infractions qui se trouvent sur le territoire de

la Partie dont ils ont la nationalité peuvent éviter d'avoir à répondre d'une infraction commise dans une autre Partie à moins que les autorités locales ne soient obligées d'intervenir. En application du paragraphe 6, si une autre Partie a demandé l'extradition du délinquant et que celle-ci a été refusée parce que la personne en question est un ressortissant de la Partie requise, cette dernière doit, à la demande de la Partie requérante, soumettre l'affaire à ses autorités compétentes aux fins de poursuites. Si la Partie dont la demande d'extradition a été rejetée ne demande pas que l'affaire soit soumise à ces autorités aux fins d'enquête et de poursuites, la partie requise n'est pas tenue d'intervenir. De plus, si aucune demande d'extradition n'a été présentée ou que l'extradition a été refusée pour une raison autre que la nationalité, ce paragraphe ne fixe pour la Partie requise aucune obligation de saisir les autorités locales aux fins de poursuites. En outre, le paragraphe 6 impose que l'enquête et les poursuites locales soient menées avec célérité ; elles doivent l'être avec le même sérieux que « pour toute autre infraction de nature comparable » qui serait instruite dans la Partie saisissant ses autorités. Cette Partie rend compte de l'issue de l'enquête et de la procédure à la Partie requérante.

252. Afin que chaque Partie sache à qui adresser ses demandes d'arrestation provisoire ou d'extradition, le paragraphe 7 oblige les Parties, en l'absence de traité, à communiquer au Secrétaire général du Conseil de l'Europe le nom et l'adresse de leurs autorités responsables de l'envoi ou de la réception des demandes d'extradition ou d'arrestation provisoire. L'application de cette disposition est limitée aux cas où aucun traité n'a été conclu entre les Parties concernées. En effet, si un traité d'extradition bilatéral ou multilatéral est en vigueur entre les Parties (tel que le STE n° 24), celles-ci savent à qui adresser les demandes d'extradition ou d'arrestation provisoire sans qu'il soit besoin de tenir le registre des autorités concernées. La communication au Secrétaire général doit être faite au moment de la signature ou du dépôt par la Partie de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion. Il convient de noter que la désignation d'une autorité n'exclut pas la possibilité de recourir à la voie diplomatique.

Titre 3 – Principes généraux relatifs à l'entraide

Principes généraux relatifs à l'entraide (article 25)

253. Les principes généraux régissant l'obligation d'entraide sont énoncés au paragraphe 1. L'entraide « la plus large possible » doit être accordée. De la sorte, comme à l'article 23 (« Principes généraux relatifs à la coopération internationale »), l'entraide doit en principe être étendue et les entraves

dont elle peut faire l'objet doivent être strictement limitées. En second lieu, comme à l'article 23, l'obligation de coopérer s'applique en principe à la fois aux infractions pénales liées à des systèmes et des données informatiques (c'est-à-dire aux infractions visées à l'article 14, paragraphe 2, *lettres a et b*) et à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. Il a été décidé d'imposer une obligation de coopérer au titre de cette vaste catégorie d'infractions car il y a lieu de rationaliser les mécanismes de la coopération internationale dans ces deux domaines. Toutefois, les articles 34 et 35 autorisent les Parties à modifier le champ d'application de ces mesures.

254. D'autres dispositions du présent chapitre précisent que l'obligation de s'accorder l'entraide doit généralement être remplie conformément aux clauses des traités, lois et accords d'entraide applicables. En vertu du paragraphe 2, chaque Partie est tenue de mettre en place les fondements juridiques qui lui permettront d'accorder les formes spécifiques de coopération décrites dans la suite du chapitre, si ses traités, lois et accords ne contiennent pas déjà des dispositions de ce genre. L'existence de ces mécanismes, en particulier de ceux dont il est question dans les articles 29 à 35 (Dispositions spécifiques – Titres 1, 2, 3), est indispensable à l'organisation d'une coopération efficace dans les affaires pénales en relation avec l'ordinateur.

255. Certaines Parties n'auront pas besoin d'adopter de mesures législatives particulières afin d'appliquer les dispositions visées au paragraphe 2, car les clauses des traités internationaux qui instituent des régimes détaillés d'entraide sont considérés comme ayant automatiquement force de loi. On compte que les Parties soit pourront considérer ces dispositions comme ayant automatiquement force de loi, soit disposeront déjà d'une législation d'entraide suffisamment souple pour leur permettre de s'acquitter des mesures d'entraide instituées en application de ce chapitre, soit pourront adopter rapidement les mesures législatives nécessaires à cette fin.

256. Les données informatiques sont très volatiles. Il suffit de presser sur quelques touches ou d'utiliser un programme automatique pour les effacer, ce qui rend impossible de remonter jusqu'à l'auteur d'une infraction ou détruit les preuves de sa culpabilité. Certains types de données ne sont stockés que pour de courtes périodes avant d'être détruites. Dans d'autres cas, si des preuves ne sont pas recueillies rapidement, des personnes ou des biens peuvent subir un préjudice important. Dans des situations aussi urgentes, la demande comme la réponse doivent être rapides. L'objet du paragraphe 3 consiste donc à faciliter l'accélération du processus visant à garantir l'entraide pour éviter que des informations ou des preuves essentielles ne soient perdues parce qu'elles

auraient été effacées avant qu'une demande d'entraide n'ait pu être préparée et transmise et qu'une réponse n'ait pu être reçue. Le paragraphe 3 atteint ce résultat 1) en autorisant les Parties à présenter, en cas d'urgence, une demande de coopération par des moyens rapides de communication, et non par les moyens classiques beaucoup plus lents de transmission de documents écrits sous pli cacheté par la valise diplomatique ou par la poste ; et 2) en imposant à la Partie requise de répondre à une telle demande par des moyens rapides de communication. Chaque Partie est tenue de se donner les moyens d'appliquer cette mesure si elle n'est pas déjà prévue dans ses traités, lois ou accords d'entraide. La télécopie et le courrier électronique sont mentionnés à titre purement indicatif : tout autre moyen rapide de communication, adapté aux circonstances de l'espèce, peut être utilisé. Les progrès technologiques pourront offrir d'autres moyens rapides de communication qui pourront servir à faire une demande d'entraide. S'agissant de la règle concernant les conditions d'authenticité et de sécurité, les Parties peuvent arrêter d'un commun accord les modalités d'authentification des communications et les garanties de sécurité spéciales (y compris le cryptage) qui pourraient s'avérer nécessaires dans des affaires particulièrement délicates. Enfin, le paragraphe autorise la Partie requise à exiger une confirmation officielle ultérieure, à transmettre par les voies classiques.

257. Le paragraphe 4 énonce le principe général selon lequel l'entraide est soumise aux conditions fixées par les traités d'entraide et les dispositions du droit interne. Ces régimes garantissent les droits des personnes se trouvant sur le territoire de la Partie requise pouvant faire l'objet d'une demande d'entraide. Ainsi, par exemple, une mesure intrusive telle qu'une opération de perquisition et de saisie n'est exécutée au nom d'une Partie requérante que si la Partie requise a la certitude que les conditions nécessaires à la prise d'une telle mesure dans une affaire intérieure ont été remplies. Les Parties peuvent également garantir la protection des droits des personnes en ce qui concerne les objets saisis et fournis par la voie de l'entraide judiciaire.

258. Toutefois, le paragraphe 4 ne s'applique pas en cas de « disposition contraire expressément prévue dans le présent chapitre. » Cette clause vise à indiquer que la Convention contient plusieurs dérogations importantes au principe général. La première de ces dérogations découle du paragraphe 2 du présent article, en vertu duquel chaque Partie est tenue d'accorder les formes de coopération énoncées dans les autres articles du chapitre (telles que la conservation, la collecte en temps réel de données, la perquisition et la saisie et la gestion d'un réseau 24/7), indépendamment de la question de savoir si ces mesures sont déjà inscrites dans ses traités d'entraide, ses arrangements équivalents ou sa

législation en matière d'entraide. On trouve une autre dérogation à l'article 27 qui est toujours applicable à l'exécution de requêtes à la place d'une disposition du droit interne de la Partie requise régissant la coopération internationale en l'absence d'un traité d'entraide ou arrangement équivalent entre la Partie requérante et la Partie requise. L'article 27 présente un système de conditions et de motifs de refus. En vertu d'une autre dérogation, expressément prévue au paragraphe 4 de l'article 26, la Partie requise ne peut pas refuser l'entraide au moins en ce qui concerne les infractions établies conformément aux articles 2-11 de la Convention, au motif que la requête porte sur une infraction qu'elle considère comme de nature « fiscale ». Enfin, l'article 29 est une dérogation en ce sens qu'il dispose que la conservation ne peut pas être refusée pour des raisons tenant à la double incrimination, bien qu'il prévoie la possibilité de formuler une réserve à ce sujet.

259. Pour l'essentiel, le paragraphe 5 donne une définition de la double incrimination aux fins de l'entraide au sens de ce chapitre. Lorsque la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination (par exemple lorsqu'elle s'est réservé le droit d'exiger la double incrimination comme condition pour exécuter une requête de conservation des données en application du paragraphe 4 de l'article 29, « Conservation rapide de données informatiques stockées »), cette condition sera considérée comme satisfaite si le comportement constituant l'infraction en relation avec laquelle l'entraide est requise est également qualifié d'infraction pénale par le droit interne de la Partie requise, même si ledit droit interne classe l'infraction dans une catégorie d'infractions différente ou la désigne en utilisant une terminologie différente. Cette disposition a été jugée nécessaire afin de garantir que les parties requises ne recourent pas à un critère trop rigide lorsqu'elles appliquent la double incrimination. Étant donné les différences entre les ordres juridiques nationaux, on ne s'étonnera pas de constater des différences de terminologie et de classement des comportements criminels. Si le comportement constitue une infraction pénale dans les deux ordres juridiques, ces différences d'ordre technique ne devraient pas empêcher l'octroi de l'entraide. Dans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance.

Information spontanée (article 26)

260. Cet article a été établi sur la base de dispositions d'instruments antérieurs du Conseil de l'Europe telles que l'article 10 de la Convention relative au blanchiment, au dépistage, à la saisie et la confiscation des produits du crime (STE n° 141) et l'article 28 de la Convention pénale sur la corruption (STE n° 173).

Il arrive de plus en plus souvent qu'une partie possède des informations précieuses dont elle estime qu'elles pourraient présenter un intérêt pour l'enquête ou la procédure ouverte ou engagée dans une autre Partie et dont celle-ci n'a pas connaissance. En pareil cas, aucune demande d'entraide n'est présentée. Le paragraphe 1 habilite l'Etat qui possède l'information en question à la communiquer à l'autre Etat sans que celui-ci lui en ait fait la demande au préalable. On a jugé bon d'insérer cette disposition car, en application de la législation de certains Etats, une telle habilitation positive est nécessaire pour pouvoir accorder l'entraide en l'absence d'une demande. Une Partie n'est pas tenue de communiquer spontanément des informations à une autre Partie ; elle a toute latitude pour le faire en fonction des circonstances de l'espèce. De plus, la divulgation spontanée d'informations n'interdit pas à la Partie qui les communique, si elle a compétence pour le faire, d'ouvrir une enquête ou d'engager une procédure au sujet des faits ainsi divulgués.

261. Le paragraphe 2 traite du fait que dans certains cas, une Partie ne communiquera spontanément des informations que si les informations sensibles restent confidentielles ou si elles sont utilisées sous certaines autres conditions. En particulier, la confidentialité sera un facteur important dans les affaires où d'importants intérêts de l'Etat communiquant les informations pourraient être mis en péril si celles-ci étaient rendues publiques, par exemple s'il y a lieu de ne pas révéler une méthode de collecte de l'information ou le fait qu'une association de malfaiteurs fait l'objet d'une enquête. Si, renseignements pris au préalable, il s'avère que la Partie destinataire ne peut pas respecter la condition mise par l'autre Partie à l'utilisation des informations (si, par exemple, elle ne peut pas respecter à la demande de confidentialité parce que les informations en questions doivent être utilisées à titre de preuves lors d'un procès public), elle doit en informer l'autre Partie, qui peut alors décider de communiquer ces informations ou de ne pas le faire. Si, toutefois, la Partie destinataire accepte la condition fixée, elle doit s'y plier. On prévoit que les conditions imposées par cet article seraient compatibles avec celle que pourrait fixer la Partie communiquant les informations à la suite d'une demande d'entraide présentée par la Partie destinataire.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables (article 27)

262. L'article 27 oblige les Parties à appliquer certaines procédures et conditions d'entraide lorsqu'il n'existe pas de traité d'entraide ni d'arrangement

établi sur la base des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise. L'article renforce donc le principe général suivant lequel l'entraide doit être mise en œuvre en appliquant les traités correspondants ou des arrangements analogues d'entraide. Les auteurs de la Convention n'ont pas voulu créer un régime général d'entraide distinct qui se substituerait aux autres instruments et arrangements applicables, estimant qu'il serait plus commode de s'en remettre d'une façon générale aux régimes fixés par les traités d'entraide en vigueur, ce qui permet aux spécialistes de l'entraide d'utiliser des instruments et arrangements qu'ils connaissent bien en évitant tout risque de confusion qui pourrait résulter de la mise en place de régimes concurrents. Comme on l'a déjà indiqué, les mécanismes dont le besoin se fait tout particulièrement sentir pour permettre une entraide efficace rapide en matière de criminalité informatique, comme ceux que prévoient les articles 29 à 35 (Dispositions spécifiques – Titres 1, 2, 3) sont les seuls au titre desquels chaque Partie est tenue de mettre en place les fondements juridiques lui permettant d'accorder les formes d'entraide voulues si ses traités, arrangements ou lois d'entraide en vigueur ne contiennent pas de dispositions en ce sens.

263. Il s'ensuit que la plupart des formes d'entraide visées dans le présent chapitre continueront d'être accordées en vertu de la Convention européenne d'entraide judiciaire en matière pénale (STE n° 30) et de son Protocole (STE n° 99) entre Parties à ces instruments. Selon une autre formule, les Parties à la présente Convention qui ont signé des traités bilatéraux d'entraide ou des accords multilatéraux d'entraide en matière pénale (tels que les accords liant les Etats membres de l'Union européenne) continueront d'en appliquer les clauses, complétées par les mécanismes applicables à la criminalité informatique ou en relation avec l'ordinateur décrits dans le reste du chapitre III, à moins qu'elles ne décident d'appliquer à la place tout ou partie du reste de cet article. L'entraide peut également découler d'arrangements établis sur la base de législations uniformes ou réciproques, tels que le système de coopération instauré entre les pays nordiques, qui est également reconnu par la Convention européenne d'entraide judiciaire en matière pénale (article 25, paragraphe 4) et le système instauré entre les membres du Commonwealth. Enfin, la référence aux traités d'entraide ou arrangements établis sur la base des législations uniformes ou réciproques n'est pas limitée aux instruments en vigueur au moment de l'entrée en vigueur de la présente Convention, mais concerne également les instruments qui pourront être adoptés ultérieurement.

264. Les paragraphes 2 à 10 de l'article 27 (Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables) prévoient un

certain nombre de règles régissant l'octroi d'une entraide en l'absence d'un traité d'entraide ou d'un arrangement établi sur la base de législations uniformes ou réciproques, parmi lesquelles la création d'une autorité centrale, l'imposition de conditions, motifs et procédures en cas d'ajournement ou de refus, la confidentialité des requêtes et les communications directes. En ce qui concerne ces questions expressément traitées, en l'absence d'un traité d'entraide ou d'un arrangement établi sur la base des législations uniformes ou réciproques, les dispositions de cet article doivent se substituer aux dispositions de droit interne régissant normalement l'entraide. D'un autre côté, l'article 27 n'offre pas de règles concernant d'autres questions le plus souvent abordées dans la législation nationale régissant l'entraide internationale. Ainsi, par exemple, on n'y trouve aucune disposition concernant la forme et le contenu des requêtes, l'audition de témoins dans les parties requise ou requérante, l'établissement de documents officiels, le transfert de témoins incarcérés ou l'assistance en matière de confiscation. En ce qui concerne ces questions, il découle du paragraphe 4 de l'article 25 qu'en l'absence d'une disposition spécifique dans le présent chapitre, c'est le droit interne de la Partie requise qui fixe les modalités précises de l'octroi de ce type d'entraide.

265. Le paragraphe 2 requiert la création d'une ou de plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre. L'institution d'autorités centrales, qui figure très souvent dans les instruments modernes d'entraide en matière pénale, est des plus utiles pour assurer le type de riposte rapide qui est si important dans la lutte contre la criminalité informatique ou en relation avec l'ordinateur. En premier lieu, la transmission directe d'une demande entre ces autorités est plus rapide et efficace que la transmission par la voie diplomatique. Ensuite, ces autorités veillent à ce qu'il soit donné suite avec diligence aux demandes qu'elles adressent ou qu'elles reçoivent, et s'assurent que les responsables de l'application des lois dans le pays partenaire sont informés de la meilleure façon de tenir compte des règles juridiques en vigueur dans la partie requise et qu'il est donné suite comme il convient aux requêtes particulièrement urgentes ou délicates.

266. Les parties sont invitées, pour des raisons d'efficacité, à désigner une autorité centrale unique aux fins de l'entraide ; le mieux serait, d'une façon générale, que l'autorité désignée à cette fin en vertu d'un traité d'entraide ou du droit interne d'une Partie serve également d'autorité centrale aux fins de l'application de cet article. Mais une Partie peut, si elle le souhaite, désigner plusieurs autorités centrales dès l'instant que son système d'entraide le permet. La Partie qui a créé plusieurs autorités centrales doit s'assurer que chacune

d'entre elles interprète de la même manière les dispositions de la Convention et traite rapidement et efficacement tant les demandes qu'elle reçoit que celles qu'elle envoie. Chaque partie communique au Secrétaire général du Conseil de l'Europe les noms et adresses (y compris l'adresse électronique et le numéro de télécopieur) de l'autorité et des autorités qu'elle a désignées pour recevoir des demandes d'entraide en vertu de cet article ou répondre à de telles demandes, et les Parties sont tenues de veiller à ce que la désignation soit à tout moment correcte.

267. L'un des principaux objectifs que cherche à atteindre un Etat qui requiert l'entraide est souvent d'assurer le respect des dispositions de son droit interne qui régissent l'admissibilité des preuves, ce qui lui permet d'utiliser lesdites preuves en justice. Pour qu'il puisse être donné suite à ces règles de preuve, le paragraphe 3 oblige la Partie requise à exécuter les demandes conformément à la procédure spécifiée par la Partie requérante, à moins que cette procédure ne soit incompatible avec sa législation. Soulignons que ce paragraphe ne vise que l'obligation de respecter des règles de procédure techniques et ne concerne pas les garanties de procédure fondamentales. Ainsi, par exemple, une Partie requérante ne peut pas demander à la partie requise d'exécuter une opération de perquisition et saisie qui ne serait pas conforme aux règles juridiques fondamentales appliquées par la Partie requise à ce type d'opération. Compte tenu de la nature limitée de l'obligation, il a été décidé que le simple fait qu'une telle procédure soit étrangère à l'ordre juridique de la partie requise ne constituait pas un motif suffisant pour refuser d'appliquer la procédure requise par la Partie requérante ; la procédure doit être incompatible avec les principes juridiques de la Partie requise. Ainsi, par exemple, la loi de la Partie requérante peut exiger, au plan de la procédure, qu'un témoin fasse sa déposition sous serment. Même si son droit interne n'exige pas que les témoins déposent sous serment, la Partie requise doit faire droit à la demande de la Partie requérante.

268. Le paragraphe 4 prévoit la possibilité de refuser d'exécuter les demandes d'entraide présentées en application de cet article. L'entraide peut être refusée pour les motifs visés au paragraphe 4 de l'article 25 (c'est-à-dire les motifs prévus par le droit interne de la Partie requise), y compris l'atteinte à la souveraineté de l'Etat, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels, et lorsque la Partie requise considère l'infraction comme politique ou liée à une infraction politique. Au nom du principe supérieur consistant à accorder l'entraide la plus large possible (voir articles 23 et 25), les motifs de refus établis par une Partie requise doivent être limités et invoqués avec modération. Ils ne

doivent pas prendre une ampleur telle qu'ils risqueraient d'aboutir à un refus d'entraide ou à l'octroi d'une entraide assortie de conditions trop lourdes au titre de vastes catégories de preuves ou d'informations.

269. Conformément à cette approche, il a été convenu que, outre les motifs de refus visés à l'article 28, le refus d'entraide au motif de la protection des données ne peut être invoqué que dans des cas exceptionnels. Une telle situation pourrait se présenter lorsque, après avoir pesé les intérêts importants impliqués dans un cas particulier (d'une part les intérêts publics, y compris la bonne administration de la justice et, d'autre part, des intérêts liés à la vie privée), il apparaît que la communication des données spécifiées, recherchées par la Partie requérante, soulèverait des problèmes d'une telle ampleur que la Partie requise pourrait les considérer comme relevant de motifs de refus fondés sur ses intérêts essentiels. Une application large, catégorique ou systématique des principes de protection des données pour refuser la coopération n'est, par conséquent, pas permise. Ainsi, le fait que les Parties concernées disposent de systèmes différents de protection du caractère privé des données (par exemple, la Partie requérante ne dispose pas de l'équivalent d'une autorité spécialisée en matière de protection des données) ou emploient des moyens différents pour protéger les données à caractère personnel (par exemple, la Partie requérante utilise des moyens autres que la procédure de suppression des données pour protéger le caractère privé ou l'exactitude des données à caractère personnel reçues par les autorités chargées de l'application de la loi), ne constitue pas, en soi, un motif de refus. Avant d'invoquer les « intérêts essentiels » comme motif pour refuser la coopération, la Partie requise devrait, à la place, essayer de fixer des conditions qui permettraient le transfert des données (voir Article 27, paragraphe 6 et paragraphe 271 de ce rapport).

270. Le paragraphe 5 permet à la Partie requise d'ajourner, non de refuser, l'exécution d'une demande d'entraide si l'exécution immédiate des mesures visées par la demande risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités. Ainsi, par exemple, si la Partie requérante a demandé la communication de preuves ou la déposition d'un témoin aux fins d'enquête ou de procès, et que les mêmes preuves ou dépositions sont nécessaires au déroulement d'un procès sur le point de commencer dans la Partie requise, celle-ci pourra valablement surseoir à l'exécution desdites mesures.

271. Le paragraphe 6 dispose que dans les cas où elle serait normalement amenée à refuser ou ajourner sa coopération, la Partie requise peut l'assortir

de conditions. Si celles-ci ne conviennent pas à la Partie requérante, la Partie requise peut les modifier ou se prévaloir de son droit de refuser sa coopération ou d'y surseoir. Etant donné que la Partie requise est tenue d'accorder la coopération la plus large possible, il a été décidé qu'elle devrait utiliser avec modération son droit de refus et celui de fixer des conditions.

272. Le paragraphe 7 oblige la Partie requise d'informer la Partie requérante de la suite qu'elle entend donner à sa demande d'entraide et de motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de l'entraide. Le fait que la Partie requise doit indiquer ses raisons peut, entre autres, aider la Partie requérante à comprendre comment la Partie requise interprète les exigences de cet article, fournit une base en vue des consultations qui pourraient être engagées pour améliorer l'efficacité de l'entraide et permet à la Partie requérante d'avoir accès à des informations factuelles dont elle n'avait pas eu connaissance concernant l'existence ou la situation de témoins ou de preuves.

273. Il peut arriver qu'une Partie fasse une demande d'entraide à propos d'une affaire très délicate ou d'une affaire pour laquelle la divulgation prématurée des faits ayant motivé la requête pourrait avoir des conséquences désastreuses. Le paragraphe 8 autorise donc la Partie requérante à demander à la Partie requise de s'assurer que le fait et l'objet de la requête restent confidentiels. Toutefois, la confidentialité ne peut être sollicitée que dans la mesure où elle n'empêche pas la Partie requise d'obtenir les preuves ou les informations demandées ; or, il peut arriver, par exemple, que la divulgation des informations en question soit indispensable pour obtenir une ordonnance judiciaire aux fins d'exécution de la demande d'entraide, ou qu'il faille notifier la requête à des particuliers ayant des preuves en leur possession pour que cette requête puisse être exécutée. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer la Partie requérante, qui aura alors la possibilité de retirer sa demande ou de la modifier.

274. Les autorités centrales désignées conformément au paragraphe 2 communiquent directement entre elles. Toutefois, en cas d'urgence, les juges et procureurs de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide judiciaire. Le juge ou le procureur appliquant cette procédure doit également adresser une copie de la demande à l'autorité centrale de son pays, à charge pour celle-ci de la transmettre à l'autorité centrale de la Partie requise. En vertu de la lettre b) du paragraphe 9, les demandes peuvent être transmises par l'intermédiaire d'Interpol. Les autorités de la Partie requise qui reçoivent une

demande ne relevant pas de leur compétence doivent, en application de la lettre c) du paragraphe, honorer une double obligation. Premièrement, elles doivent transmettre la demande à l'autorité compétente de la Partie requise. Deuxièmement, elles doivent en informer les autorités de la Partie requérante. Conformément à la lettre d), les demandes peuvent également être transmises directement, sans l'intervention des autorités centrales, même si elles n'ont pas de caractère d'urgence, dès l'instant que l'autorité de la Partie requise peut faire droit à la demande sans avoir besoin de prendre de mesures de coercition. Enfin, la lettre e) habilite une Partie à informer les autres, par l'intermédiaire du Secrétaire général du Conseil de l'Europe, que, pour des raisons d'efficacité, les demandes doivent être adressées directement à l'autorité centrale.

Confidentialité et restriction d'utilisation (article 28)

275. Cette disposition prévoit expressément des restrictions à l'utilisation d'informations ou de matériel, de façon à permettre à la Partie requise, dans les cas où ces informations ou ce matériel sont de nature particulièrement délicate, de s'assurer que leur utilisation est limitée à celle en vue de laquelle l'entraide est accordée, ou qu'ils ne seront diffusés qu'aux services chargés de l'application de la loi de la Partie requérante. Ces restrictions constituent des garanties qui sont, entre autres, applicables aux fins de la protection des données.

276. Comme l'article 27, l'article 28 ne s'applique que lorsqu'il n'existe pas de traité d'entraide ou d'arrangement reposant sur une législation uniforme ou réciproque en vigueur entre la partie requérante et la Partie requise. Lorsqu'un tel traité ou arrangement est en vigueur, ses dispositions touchant la confidentialité et les restrictions d'utilisation s'appliquent à la place des dispositions de cet article, à moins que les Parties audit traité ou arrangement en décident autrement. On évite ainsi tout chevauchement avec des traités d'entraide juridique bilatéraux et multilatéraux existants et des arrangements analogues, ce qui permet aux praticiens de continuer d'appliquer le régime habituel au lieu de chercher à appliquer deux instruments concurrents pouvant, éventuellement, se révéler contradictoires.

277. Le paragraphe 2 permet à la Partie requise, lorsqu'elle fait droit à une demande d'entraide, de fixer deux types de conditions. Premièrement, elle peut demander que les informations ou le matériel fournis restent confidentiels lorsque la demande ne pourrait être respectée en l'absence de cette condition, comme dans le cas de l'identité d'un informateur qui doit rester

confidentielle. Il n'est pas approprié d'exiger une confidentialité absolue dans les affaires où la Partie requise est tenue de fournir l'aide demandée, car cela aboutirait souvent à gêner la Partie requérante dans la conduite de l'enquête ou de la procédure, par exemple en l'empêchant d'utiliser les éléments de preuve dans un procès public (y compris la divulgation obligatoire).

278. Deuxièmement, la Partie requise peut subordonner la communication d'informations ou de matériel à la condition qu'ils ne servent pas aux fins d'enquêtes ou de procédures autres que celles indiquées dans la requête. Cette condition ne peut s'appliquer que si son application est expressément demandée par la Partie requise ; à défaut, la Partie requérante n'est pas tenue de respecter cette restriction à l'utilisation. Dans les cas où la Partie requise demande l'application de cette restriction, celle-ci garantit que les informations et le matériel ne pourront être utilisés qu'aux fins prévues dans la demande, excluant ainsi la possibilité qu'ils le soient à d'autres fins sans le consentement de la Partie requise. Les négociateurs ont prévu deux exceptions à la capacité de restreindre l'utilisation des informations, exceptions que le libellé du paragraphe fait ressortir de façon implicite. Premièrement, conformément aux principes juridiques fondamentaux de nombreux Etats, si le matériel transmis constitue des éléments de preuve disculpant un accusé, il doit être révélé à la défense ou à une autorité judiciaire. En outre, la plupart du matériel fourni dans le cadre des accords d'entraide est destiné à une utilisation lors de procès, normalement dans le cadre d'une procédure publique (y compris la divulgation obligatoire). Une fois qu'il a été divulgué, ce matériel tombe pour l'essentiel dans le domaine public. Dans ces situations, il n'est pas possible de garantir la confidentialité aux fins d'enquêtes ou de procédures pour lesquelles l'entraide a été demandée.

279. Le paragraphe 3 dispose que, si la Partie qui a demandé communication d'informations ne peut satisfaire à l'une des conditions imposées, elle en informe la Partie appelée à fournir ces informations, qui décide alors si elle va les fournir. Si la Partie destinataire accepte cette condition, elle sera liée par elle.

280. Le paragraphe 4 dispose qu'il peut être demandé à la Partie requérante de communiquer des précisions quant à l'usage fait des informations ou du matériel qu'elle a reçus aux conditions énoncées au paragraphe 2, de sorte que la Partie requise puisse vérifier que ces conditions ont été respectées. Il a été décidé que celle-ci ne peut pas demander la communication de précisions par trop contraignantes, comme l'indication de toutes les fois où le matériel ou les informations fournis ont été consultés.

Section 2 – Dispositions spécifiques

281. La présente Section a pour objet d'instituer des mécanismes spécifiques permettant de prendre des mesures internationales efficaces et concertées dans des affaires portant sur des infractions informatiques et des preuves existant sous forme électronique.

Titre 1 – Entraide en matière de mesures provisoires

Conservation rapide de données informatiques stockées (article 29)

282. Cet article institue au niveau international un mécanisme équivalent à celui que prévoit l'article 16 au niveau national. Le paragraphe 1 de cet article autorise une Partie à demander, et le paragraphe 3 impose à chaque Partie de se donner les moyens juridiques d'obtenir, la conservation rapide de données stockées au moyen d'un système informatique sur le territoire de la Partie requise, afin que les données ne soient pas modifiées, enlevées ou effacées pendant la période nécessaire à la préparation, à la transmission et à l'exécution d'une demande d'entraide aux fins d'obtention des données. La conservation est une mesure limitée de caractère provisoire destinée à intervenir de façon beaucoup plus rapide que l'exécution d'une requête d'entraide classique. Comme on l'a déjà indiqué, les données informatiques sont des plus volatiles. Il suffit de presser sur quelques touches ou d'utiliser des programmes automatiques pour les effacer, les modifier ou les déplacer, ou pour rendre impossible de remonter jusqu'à l'auteur de l'infraction constatée, voire pour détruire les preuves décisives de sa culpabilité. Certains types de données informatiques ne sont stockés que pour de brèves périodes avant d'être effacées. Il a donc été décidé qu'il fallait instituer un mécanisme qui garantirait la disponibilité de ces données pendant le déroulement du processus long et complexe de l'exécution d'une requête officielle d'entraide, qui peut s'étaler sur des semaines ou des mois.

283. Plus rapide que la méthode d'entraide habituelle, cette mesure est en même temps moins intrusive. Il n'est pas demandé aux responsables de l'entraide de la Partie requise d'obtenir la possession des données auprès de leur gardien. On juge préférable que la Partie requise s'assure que le gardien (qui est souvent un fournisseur de services ou une autre tierce partie) conserve (c'est-à-dire n'efface pas) les données en attendant que soit ordonnée leur remise ultérieure aux services chargés de l'application de la loi. Cette procédure a l'avantage d'être rapide et de respecter le droit de la personne concernée au respect de sa vie privée, car les données ne seront divulguées

à un fonctionnaire quelconque ou examinées par celui-ci que lorsqu'il aura été satisfait aux critères applicables à la divulgation intégrale en conformité avec les accords d'entraide normaux. D'un autre côté, une Partie requise est autorisée à utiliser d'autres procédures pour garantir la conservation rapide des données, y compris la délivrance et l'exécution accélérées d'une injonction de produire ou d'un mandat de perquisition. L'élément primordial est de pouvoir engager un processus extrêmement rapide pour empêcher les données d'être perdues à jamais.

284. Le paragraphe 2 énonce la teneur d'une demande de conservation aux fins de cet article. Etant donné qu'il s'agit d'une mesure provisoire et qu'une telle demande doit être préparée et transmise rapidement, les informations seront présentées sous forme résumée et ne porteront que sur les éléments minimaux requis pour permettre la conservation des données. En sus de l'identification de l'autorité qui demande la conservation et de l'infraction à l'origine de la demande, cette dernière doit fournir un bref exposé des faits, des indications suffisantes pour identifier les données à conserver et déterminer leur emplacement, et pour montrer le lien existant entre ces données et l'enquête ou la poursuite engagée au titre de l'infraction en question, ainsi que la nécessité de la mesure de conservation. Enfin, la Partie requérante doit s'engager à soumettre ultérieurement une demande d'entraide de façon à pouvoir obtenir la production des données.

285. Le paragraphe 3 énonce le principe selon lequel la double incrimination n'est pas requise comme condition préalable à la conservation. D'une façon générale, l'application du principe de la double incrimination est contre-productive en matière de conservation. Tout d'abord, du point de vue de la pratique contemporaine de l'entraide, on constate une tendance à éliminer la règle de la double incrimination pour toutes les mesures procédurales sauf les plus intrusives, telles que la perquisition et la saisie ou l'interception. Or, telle que l'ont conçue les auteurs de la Convention, la conservation n'est pas particulièrement intrusive dans la mesure où le gardien ne fait que maintenir la possession de données se trouvant légalement en sa possession et où les données ne sont divulguées aux responsables de la Partie requise ou examinées par eux qu'après l'exécution d'une demande d'entraide officielle visant leur divulgation. Ensuite, d'un point de vue pratique, il faut souvent tant de temps pour obtenir les éclaircissements nécessaires en vue d'établir de façon irréfutable l'existence de la double incrimination que les données pourraient être effacées, déplacées ou modifiées avant qu'elle puisse être établie. Ainsi, par exemple, aux premières étapes d'une enquête, la Partie requérante peut

s'apercevoir qu'une intrusion dans un ordinateur se trouvant sur son territoire s'est produite, mais peut ne comprendre que plus tard la nature et l'étendue des dommages. Si la Partie requise devait ajourner la conservation des données relatives au trafic qui permettraient de remonter à la source de l'intrusion jusqu'à ce que la double incrimination ait été établie de façon irréfutable, les données décisives seraient souvent effacées par les fournisseurs de services qui ne les conservent généralement que pendant quelques heures ou quelques jours après la transmission de la communication. Même si, par la suite, la Partie requérante était capable d'établir la double incrimination, les données décisives relatives au trafic ne pourraient pas être récupérées et l'auteur de l'infraction ne serait jamais identifié.

286. En conséquence, les parties doivent, en règle générale, renoncer à exiger la double incrimination aux fins de la conservation. Toutefois, le paragraphe 4 institue une réserve limitée. Si une Partie exige la double incrimination comme condition pour répondre à une demande d'entraide visant la production de données et qu'elle a des raisons de penser qu'au moment de la divulgation, la condition de la double incrimination ne pourra être remplie, elle peut se réserver le droit d'exiger la double incrimination comme condition préalable à la conservation. S'agissant des infractions établies conformément aux articles 2 à 11, on part du principe que la condition de la double incrimination est automatiquement remplie, sauf dispositions contraires figurant dans les réserves, prévues par la Convention, que les Parties peuvent avoir formulées au sujet de ces infractions. Par conséquent, les Parties ne peuvent imposer cette condition que vis-à-vis d'infractions autres que celles qui sont définies dans la Convention.

287. Pour le reste, conformément au paragraphe 5, la Partie requise ne peut refuser la demande de conservation que si son exécution risque de porter préjudice à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels, ou si elle considère l'infraction comme étant de nature politique ou comme étant liée à une infraction de nature politique. Cette mesure étant jugée indispensable pour l'efficacité de l'instruction et de la poursuite des infractions informatiques ou en relation avec l'ordinateur, il a été décidé d'interdire d'arguer de tout autre motif pour refuser une demande de conservation.

288. Il arrive que la Partie requise se rende compte que le gardien des données risque d'intervenir d'une façon qui compromette la confidentialité de l'enquête de la Partie requérante ou nuise d'une autre façon à celle-ci (par exemple lorsque les données à conserver sont sous la garde d'un fournisseur de services contrôlé par une organisation criminelle ou par la cible de l'enquête

elle-même). En pareil cas, en vertu du paragraphe 6, la Partie requérante doit être rapidement informée, de sorte qu'elle puisse déterminer si elle peut prendre le risque que présente l'exécution de la requête de conservation ou s'il vaut mieux utiliser une forme plus intrusive mais plus sûre d'entraide, telle que l'injonction de produire ou la perquisition et la saisie.

289. Enfin, le paragraphe 7 oblige chaque Partie à faire en sorte que les données conservées en application de cet article le soient pour une période d'au moins 60 jours en attendant la réception de la demande d'entraide officielle visant leur divulgation et continuent d'être conservées après la réception de la demande.

Divulgation rapide de données conservées (article 30)

290. Cet article institue au niveau international l'équivalent des pouvoirs établis au niveau national par l'article 17. Il arrive souvent qu'à la demande d'une Partie dans laquelle une infraction a été commise, une Partie requise conserve les données relatives au trafic concernant la transmission d'une communication par ses ordinateurs afin de pouvoir remonter à la source de la communication et identifier l'auteur de l'infraction, ou localiser des preuves décisives. Ce faisant, la Partie requise peut s'apercevoir que les données relatives au trafic découvertes sur son territoire montrent que la communication a été acheminée par un fournisseur de services d'un Etat tiers ou par un fournisseur se trouvant dans la Partie requérante elle-même. En pareil cas, la Partie requise doit fournir rapidement à la Partie requérante une quantité suffisante de données relatives au trafic pour permettre d'identifier le fournisseur de services de l'Etat tiers et la voie par laquelle la communication a été transmise par celui-ci. Si la communication a été transmise depuis un Etat tiers, ces informations permettent à la Partie requérante d'adresser à ce dernier une demande de conservation et d'entraide accélérée visant à remonter à la véritable source de la communication. Si la communication a été retransmise vers la Partie requérante, elle peut obtenir la conservation et la divulgation de nouvelles données relatives au trafic par le jeu des procédures nationales.

291. En vertu du paragraphe 2, la Partie requise ne peut refuser la divulgation de données relatives au trafic que si celle-ci risque de porter préjudice à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels, ou si elle considère l'infraction comme étant de nature politique ou liée à une infraction de nature politique. Comme pour l'article 29 (Conservation rapide de données informatiques stockées), ce type d'informations étant si important pour pouvoir identifier les auteurs d'infractions au sens de la Convention ou

localiser des preuves décisives, les motifs de refus doivent être strictement limités, et il a été décidé d'interdire d'arguer de tout autre motif pour refuser une demande de divulgation.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Entraide concernant l'accès aux données stockées (article 31)

292. Chaque partie doit avoir la capacité, au bénéfice de l'autre, de perquisitionner ou d'accéder par un moyen similaire, de saisir ou d'obtenir par un moyen similaire, et de divulguer des données stockées au moyen d'un système informatique se trouvant sur son territoire – tout comme elle doit, en vertu de l'article 19 (Perquisition et saisie de données informatiques stockées), avoir la capacité de le faire à des fins nationales. Le paragraphe 1 autorise une Partie à demander ce type d'entraide et le paragraphe 2 exige de la Partie requise qu'elle se donne les moyens de la fournir. Par ailleurs, le paragraphe 2 est conforme au principe selon lequel les conditions dans lesquelles cette coopération doit être fournie sont celles qu'énoncent les traités, arrangements et législations nationales applicables concernant l'entraide judiciaire en matière pénale. En vertu du paragraphe 3, il doit être satisfait rapidement à une telle demande lorsque 1) il y a des raisons de penser que les données pertinentes sont particulièrement susceptibles de perte ou de modification, ou 2) les traités, arrangements ou législations prévoient une coopération rapide.

Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public (article 32)

293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des Etats agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret ; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire

figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. A cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.

294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations : d'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne « légalement autorisée » pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par exemple, le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article.

Entraide dans la collecte en temps réel de données relatives au trafic (article 33)

295. Très souvent, les enquêteurs ne peuvent être sûrs de pouvoir remonter à la source d'une communication en se fiant aux enregistrements des transmissions antérieures car des données relatives au trafic cruciales peuvent avoir été automatiquement effacées par un fournisseur de services de la filière de transmission avant de pouvoir être conservées. Il est donc indispensable que les enquêteurs de chaque Partie puissent avoir la possibilité de se procurer en temps réel des données relatives au trafic concernant des communications transmises par un système informatique se trouvant sur le territoire d'autres Parties. En conséquence, en vertu de l'article 33 (Entraide dans la collecte en temps réel de données relatives au trafic), chaque Partie est tenue de collecter en temps réel des données relatives au trafic pour une autre Partie. Cet article impose aux Parties de coopérer en la matière,

mais, comme pour d'autres dispositions, il est tenu compte des modalités d'entraide en vigueur, et les clauses et conditions concernant l'octroi de cette coopération sont généralement celles que prévoient les traités, arrangements et législations applicables régissant l'entraide judiciaire en matière pénale.

296. Dans maints pays, l'entraide est accordée pour l'essentiel en ce qui concerne la collecte en temps réel des données relatives au trafic, car cette collecte est jugée moins intrusive que l'interception des données relatives au contenu ou la perquisition et saisie. Mais un certain nombre d'Etats adoptent une approche plus étroite. C'est la raison pour laquelle, de la même façon que les Parties peuvent formuler une réserve au titre du paragraphe 3 de l'article 14 (Portée des mesures du droit de procédure), s'agissant de la portée de la mesure interne équivalente, le paragraphe 2 autorise les Parties à resserrer l'éventail des infractions auxquelles appliquer cette mesure au regard des dispositions de l'article 23 (Principes généraux relatifs à la coopération internationale). Le paragraphe comporte toutefois une mise en garde : en aucun cas l'éventail des infractions ne doit être plus étroit que celui des infractions pour lesquelles cette mesure est disponible dans une affaire analogue relevant du droit interne. En fait, comme la collecte en temps réel de données relatives au trafic est parfois le seul moyen d'identifier l'auteur d'une infraction et comme cette mesure a un caractère moins intrusif, l'utilisation de l'expression « au moins » au paragraphe 2 vise à encourager les Parties à autoriser l'octroi de l'entraide la plus large possible, c'est-à-dire même en l'absence de double incrimination.

Entraide en matière d'interception de données relatives au contenu (article 34)

297. Le caractère très intrusif de l'interception restreint l'obligation d'accorder l'entraide aux fins d'interception des données relatives au contenu. Cette entraide doit être accordée dans la mesure permise par les traités et lois internes applicables des Parties. La pratique de l'entraide en matière d'interception de données relatives au contenu n'en étant encore qu'à ses débuts, il a été décidé de s'en remettre aux régimes et législations internes en vigueur en matière d'entraide pour ce qui est de la portée de l'obligation d'assistance et des restrictions dont cette obligation doit faire l'objet. A cet égard, on se reportera aux commentaires concernant les articles 14, 15 et 21 ainsi qu'à la Recommandation n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications.

Titre 3 – Réseau 24/7

Réseau 24/7 (article 35)

298. Comme on l'a vu, l'efficacité de la lutte contre les infractions commises au moyen de systèmes informatiques et celle de la collecte de preuves électroniques sont liées à la rapidité d'intervention. De plus, il suffit de presser sur quelques touches pour produire des effets à des milliers de kilomètres en latitude comme en longitude. Aussi est-il nécessaire de compléter les modalités de coopération et d'entraide au niveau des services de police pour relever efficacement les défis de l'âge informatique. La modalité instituée dans cet article s'appuie sur l'expérience acquise dans l'exploitation d'un réseau existant, à savoir celui créé sous les auspices du Groupe des 8 pays les plus industrialisés. En application de cet article, chaque Partie est tenue de désigner un point de contact joignable 24 heures sur 24, sept jours sur sept, afin de fournir une assistance immédiate aux fins des investigations et des procédures à conduire dans le cadre de ce chapitre, en particulier telle qu'elle est définie aux lettres a) à c) du paragraphe 1 de l'article 35. On a considéré que la mise en place de ce réseau figure parmi les moyens les plus importants prévus par la Convention pour veiller à ce que les Parties puissent s'attaquer dans de bonnes conditions aux problèmes que la criminalité informatique et en relation avec l'ordinateur pose aux services chargés de l'application des lois.

299. Le point de contact 24/7 de chaque Partie est chargé soit de la facilitation, soit de l'application directe d'un certain nombre de mesures, parmi lesquelles l'apport de conseils techniques, la conservation des données, le recueil de preuves, l'apport d'informations à caractère juridique et la localisation des suspects. Par « informations à caractère juridique » (paragraphe 1), il faut entendre les conseils donnés à une autre Partie qui demande l'entraide au sujet de toutes conditions juridiques préalables à l'octroi d'une coopération informelle ou officielle.

300. Chaque Partie a toute latitude pour décider de la place du point de contact 24/7 dans l'organigramme de ses services chargés de faire respecter la loi. Dans certaines Parties, il pourra relever de l'autorité centrale responsable de l'entraide ; d'autres jugeront opportun de le rattacher à un service de police spécialisé dans la lutte contre la criminalité informatique. D'autres Parties pourront avoir d'autres préférences liées à leur structure administrative et leur ordre juridique. Etant donné que le point de contact 24/7 est appelé à la fois à fournir des conseils techniques pour mettre en échec une attaque

ou déterminer l'origine d'une attaque et à accorder une coopération internationale en localisant des suspects, par exemple, il n'y a pas de solution unique et on s'attend à voir évoluer la structure du réseau avec le temps. Au moment de désigner un point de contact national, il faudra tenir dûment compte de la nécessité de communiquer avec des points de contact dans des langues étrangères.

301. Le paragraphe 2 dispose que l'une des tâches essentielles qui reviennent au point de contact 24/7 est la capacité de faciliter l'exercice rapide des fonctions qu'il n'assume pas directement lui-même. Ainsi, par exemple, si le point de contact est membre d'un service de police, il doit être capable de coordonner rapidement son action avec celle des autres services compétents au sein du gouvernement, tels que l'autorité centrale responsable de l'extradition ou de l'entraide internationale, afin que les mesures qui s'imposent puissent être prises à toute heure du jour et de la nuit. De plus, le paragraphe 2 requiert du point de contact 24/7 de chaque Partie qu'il corresponde avec les autres membres du réseau selon une procédure accélérée.

302. Le paragraphe 3 impose à chaque point de contact du réseau d'être bien équipé. Le réseau aura besoin, pour fonctionner sans à-coups, de téléphones, de télécopieurs et de matériel informatique récents ; à mesure que les technologies évoluent, d'autres types de matériels de communication et d'analyse devront être intégrés au système. Le paragraphe 3 exige également que les membres de l'équipe de chaque Partie reçoivent la formation voulue en matière de criminalité informatique et les moyens les plus efficaces de la combattre.

Chapitre IV – Clauses finales

303. A quelques exceptions près, les clauses de ce chapitre s'inspirent pour l'essentiel des « Clauses finales types pour les conventions et accords conclus dans le cadre du Conseil de l'Europe », que le Comité des Ministres a approuvées à sa 315^e Réunion des Délégués tenue en février 1980. Etant donné que la plupart des articles 36 à 48 reprennent le libellé des clauses types ou s'inspirent de la longue pratique conventionnelle du Conseil de l'Europe, ils n'appellent pas de commentaires particuliers. Toutefois, certaines modifications des clauses types ou certaines clauses nouvelles requièrent une explication. On notera à cet égard que les clauses types ont été adoptées en tant qu'ensemble non contraignant de dispositions. Comme indiqué dans l'introduction aux clauses types, « les présentes clauses finales types ne visent qu'à faciliter la tâche des comités d'experts et éviter des différences de libellé qui n'auraient aucune

justification réelle. Les clauses types ne sont nullement contraignantes : des clauses différentes peuvent être adaptées à des situations particulières.»

Signature et entrée en vigueur (article 36)

304. Le paragraphe 1 de l'article 36 a été rédigé en tenant compte de plusieurs précédents établis par d'autres conventions élaborées dans le cadre du Conseil de l'Europe, comme la Convention sur le transfèrement des personnes condamnées (STE n° 112) et la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime (STE n° 141), lesquelles peuvent être signées, avant leur entrée en vigueur, non seulement par les Etats membres du Conseil de l'Europe, mais aussi par les Etats non membres qui ont participé à leur élaboration. Cette clause vise à permettre à un maximum d'Etats intéressés, et non pas seulement les membres du Conseil de l'Europe, de devenir dès que possible Parties à ces Conventions. En l'occurrence, cette clause s'applique à quatre Etats non membres, l'Afrique du Sud, le Canada, les Etats-Unis d'Amérique et le Japon, qui ont participé activement à l'élaboration de la Convention. Une fois que la Convention sera entrée en vigueur, conformément au paragraphe 3, d'autres Etats non membres auxquels ne s'applique pas cette clause pourront être invités à adhérer à la Convention conformément au paragraphe 1 de l'article 37.

305. Le paragraphe 3 de l'article 36 fixe à 5 le nombre des ratifications, acceptations ou approbations requises pour l'entrée en vigueur de la Convention. Plus élevé que le seuil habituellement fixé (3) dans les traités du Conseil de l'Europe, ce chiffre traduit la conviction qu'un groupe d'Etats légèrement plus nombreux est nécessaire pour que l'on puisse commencer dans de bonnes conditions à relever le défi que pose la criminalité informatique mondiale. Le nombre n'est toutefois pas si élevé qu'il risque de retarder inutilement l'entrée en vigueur de la Convention. Parmi les cinq Etats originels, trois au moins doivent être membres du Conseil de l'Europe, mais les deux autres pourraient venir du groupe des quatre Etats non membres qui ont participé à l'élaboration de la Convention. Naturellement, cette clause permettrait aussi à la Convention d'entrer en vigueur si cinq Etats membres du Conseil de l'Europe exprimaient leur consentement à être liés par elle.

Adhésion à la Convention (article 37)

306. L'article 37 a également été rédigé à partir de précédents figurant dans d'autres conventions du Conseil de l'Europe, mais avec un élément supplémentaire. Conformément à une pratique déjà ancienne, le Comité des Ministres

décide, de sa propre initiative ou sur demande, après avoir consulté tous les Etats contractants, qu'il s'agisse au non d'Etats membres, d'inviter un Etat non membre, qui n'a pas participé à l'élaboration d'une convention, à y adhérer. En d'autres termes, si un Etat contractant élève une objection à l'adhésion de l'Etat non membre, le Comité des Ministres ne l'inviterait pas, en règle générale, à adhérer à la Convention. Toutefois, en vertu de la formulation habituelle, le Comité des Ministres pourrait – en principe – inviter un Etat non membre n'ayant pas participé à l'élaboration de la Convention à y adhérer même si un Etat Partie non membre élevait une objection à son adhésion. On voit que – en théorie – aucun droit de veto n'est habituellement accordé aux Etats Parties non membres dans le processus permettant à d'autres Etats non membres d'adhérer aux traités du Conseil de l'Europe. Toutefois, on a inséré une disposition explicite qui fait obligation au Comité des Ministres de consulter tous les Etats contractants à la Convention – et non pas seulement les membres du Conseil de l'Europe – et d'obtenir leur assentiment unanime avant d'inviter un Etat non membre à adhérer à la Convention. Comme on l'a vu plus haut, cette disposition est compatible avec la pratique habituelle et revient à considérer que tous les Etats contractants à la Convention doivent pouvoir décider avec quels Etats non membres établir des relations conventionnelles. Il n'en reste pas moins que la décision officielle d'inviter un Etat non membre à adhérer est prise, conformément à la pratique habituelle, par les représentants des Parties contractantes ayant le droit de siéger au Comité des Ministres. Cette décision exige une majorité des deux tiers, telle que prévue à l'article 20.d du Statut du Conseil de l'Europe, et une décision unanime des représentants des Parties contractantes ayant le droit de siéger au Comité.

Effets de la Convention (article 39)

307. Les paragraphes 1 et 2 de l'article 39 abordent la question du lien entre la Convention et d'autres accords ou arrangements internationaux. Les clauses types mentionnées plus haut ne traitent pas des liens à établir entre les conventions du Conseil de l'Europe et entre celles-ci et d'autres traités, bilatéraux ou multilatéraux, conclus en dehors du Conseil de l'Europe. En règle générale, les conventions conclues au sein du Conseil de l'Europe dans le domaine du droit pénal (comme l'Accord relatif au trafic illicite par mer (STE n° 156)), adoptent l'approche suivante : 1) les nouvelles conventions ne portent pas atteinte aux droits et engagements découlant des conventions multilatérales internationales en vigueur concernant des questions spéciales ; 2) les Parties à une nouvelle convention peuvent conclure des accords bilatéraux ou multilatéraux entre elles sur des questions traitées par la convention aux fins d'en compléter ou

renforcer les dispositions ou de faciliter l'application des principes qui y sont consacrés ; et 3) si deux ou plusieurs Parties à la nouvelle convention ont conclu un accord ou un traité relatif à une question réglée par la convention ou lorsqu'elles ont établi d'une autre manière leurs relations quant à cette question, elles auront la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention, pour autant que la coopération internationale s'en trouve facilitée.

308. Dans la mesure où la Convention, d'une façon générale, vise à compléter, non à remplacer les accords et arrangements multilatéraux et bilatéraux entre les Parties, les auteurs ont considéré que la mention, qui pourrait se révéler réductrice, de « questions spéciales » non seulement n'était pas particulièrement instructive, mais risquait d'être une source de confusion inutile. C'est pourquoi le paragraphe 1 de l'article 39 se contente d'indiquer que la présente Convention complète les autres traités ou accords applicables existant entre les Parties et il mentionne en particulier trois traités du Conseil de l'Europe parmi d'autres : la Convention européenne d'extradition de 1957 (STE n° 24), la Convention européenne d'entraide judiciaire en matière pénale de 1959 (STE n° 30) et le Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale de 1978 (STE n° 99). En conséquence, en ce qui concerne les questions générales, ces accords ou arrangements doivent en principe être appliqués par les Parties à la Convention sur la cybercriminalité. S'agissant des questions spécifiques traitées uniquement par cette Convention, la règle d'interprétation *lex specialis derogat legi generali* impose que les Parties donnent priorité aux règles contenues dans cette Convention. On peut citer l'exemple de l'article 30, qui prévoit la divulgation rapide des données relatives au trafic conservées lorsqu'elles sont nécessaires pour identifier la voie par laquelle une communication spécifiée a été transmise. Dans ce domaine spécifique, la Convention, en tant que *lex specialis*, doit fournir une règle de premier recours par rapport aux dispositions figurant dans les accords d'entraide de caractère plus général.

309. De même, les auteurs ont considéré qu'une formulation qui subordonnerait l'application d'accords en vigueur ou futurs à la condition qu'ils « renforcent » ou « facilitent » la coopération pourrait soulever des problèmes car, selon l'approche instituée au chapitre consacré à la coopération internationale, on présume que les Parties appliqueront les accords et arrangements internationaux pertinents.

310. Lorsqu'un traité ou accord d'entraide organisant la coopération existe, la présente Convention ne ferait que compléter, au besoin, les règles en vigueur.

Ainsi, par exemple, cette Convention prévoit la transmission des demandes d'entraide par des moyens rapides de communication (voir le paragraphe 3 de l'article 25) si cette possibilité n'est pas offerte par le traité ou accord initial.

311. Dans le droit fil du rôle d'appoint reconnu à la Convention et, en particulier, de son approche de la coopération internationale, le paragraphe 2 prévoit que les Parties ont également toute liberté pour appliquer les accords déjà en vigueur ou qui pourront l'être à l'avenir. On trouvera un précédent pour cette disposition dans la Convention sur le transfèrement des personnes condamnées (STE n° 12). Il ne fait aucun doute que l'on s'attend, dans le domaine de la coopération internationale, à ce que l'application d'autres accords internationaux (dont un grand nombre offrent des formules d'entraide internationale ayant depuis longtemps fait leurs preuves) stimule en fait la coopération. Conformément aux dispositions de la présente Convention, les Parties peuvent aussi décider d'appliquer ses clauses relatives à la coopération internationale à la place de ces autres accords (voir article 27.1). En pareil cas, les dispositions régissant la coopération énoncées à l'article 27 se substitueraient aux règles pertinentes desdits accords. Etant donné que la présente Convention prévoit généralement des obligations minimales, le paragraphe 2 de l'article 39 reconnaît que les Parties sont libres de décider d'honorer des obligations plus spécifiques, venant s'ajouter à celles qui sont déjà énoncées dans la Convention, lorsqu'elles établissent leurs relations concernant les questions réglées par la Convention. Toutefois, ce droit n'est pas absolu : les Parties doivent respecter les objectifs et principes de la Convention et ne peuvent donc accepter des obligations qui seraient contraires à son but.

312. Par ailleurs, les auteurs se sont accordés à reconnaître que, pour établir les relations entre la Convention et d'autres accords internationaux, les Parties pourraient également s'inspirer des dispositions pertinentes de la Convention de Vienne sur le droit des traités.

313. La Convention s'emploie à répondre à un besoin impératif d'harmonisation sans pour autant prétendre régler toutes les questions que soulève la criminalité informatique ou en relation avec l'ordinateur. Aussi le paragraphe 3 a-t-il été inséré pour qu'il soit bien clair que la Convention n'agit que sur les questions dont elle traite. Elle ne saurait donc affecter les autres droits, restrictions, obligations et responsabilités qui peuvent exister, mais qu'elle ne règle pas. On trouvera un précédent pour une telle « clause de sauvegarde » dans d'autres accords internationaux (comme la Convention des Nations Unies sur la lutte contre le financement du terrorisme).

Déclarations (article 40)

314. L'article 40 mentionne certains articles, qui concernent pour l'essentiel les infractions établies par la Convention dans la section relative au droit matériel, en vertu desquels les Parties sont autorisées à insérer certains éléments supplémentaires spécifiés qui modifient la portée desdites dispositions. Ces éléments supplémentaires ont pour objet de tenir compte de certaines différences théoriques ou juridiques, ce qui se justifie peut-être davantage dans un traité de portée mondiale que dans le contexte du seul Conseil de l'Europe. Les déclarations sont considérées comme des interprétations acceptables des dispositions de la Convention et doivent être distinguées des réserves, qui permettent à une Partie d'exclure ou de modifier l'effet juridique de certaines obligations énoncées dans la Convention. Comme il est important pour les Parties à la Convention d'avoir connaissance des éléments supplémentaires ayant pu être insérés par les autres Parties, l'article institue l'obligation de les signaler au Secrétaire général du Conseil de l'Europe au moment de la signature ou du dépôt de l'instrument de ratification, d'acceptation, d'approbation ou d'adhésion. Cette notification est particulièrement importante en ce qui concerne la définition des infractions, car la condition de double incrimination devra avoir été remplie au moment où les Parties exerceront certains pouvoirs de procédure. On n'a pas jugé nécessaire d'instituer une limite numérique aux déclarations.

Clause fédérale (article 41)

315. Conformément à l'objectif consistant à permettre à un nombre d'Etats aussi important que possible de devenir Parties à la Convention, l'article 41 autorise une réserve dont l'objectif est de trouver un arrangement concernant les difficultés que des Etats fédéraux risquent de rencontrer en raison de la répartition typique des pouvoirs entre les autorités fédérales et régionales. Il existe des précédents, en dehors du domaine du droit pénal, pour des déclarations ou réserves fédérales concernant d'autres accords internationaux¹¹. En l'occurrence, l'article 41 constate que des variations mineures d'application peuvent être induites par le droit et la pratique internes bien établis d'une Partie qui est un Etat fédéral. Ces variations doivent être fondées sur sa

11. Par exemple, la Convention relative au statut des réfugiés du 28 juillet 1951, Article 34 ; la Convention relative au statut des apatrides du 28 septembre 1954, Article 37 ; la Convention relative à la reconnaissance et la mise en application des décisions d'arbitrage étrangères du 10 juin 1958, Article 11 ; la Convention pour la protection de l'héritage culturel et naturel du monde du 16 novembre 1972, Article 34.

Constitution ou d'autres principes fondamentaux concernant la séparation des pouvoirs en matière de justice pénale entre le gouvernement central et les Etats constitutants ou autres entités territoriales d'un Etat fédéral. Il a été convenu entre les rédacteurs de la Convention que l'application de la clause fédérale n'entraînera que des variations mineures dans la mise en œuvre de la Convention.

316. Prenons l'exemple des Etats-Unis. En vertu de leur Constitution et des principes fondamentaux du fédéralisme, c'est la législation pénale fédérale qui est généralement appliquée si les actes en question ont des effets sur le commerce entre Etats constitutants ou avec l'étranger, alors que les questions moins importantes ou d'intérêt purement local relèvent depuis toujours de la juridiction des Etats constitutants. Cette approche du fédéralisme permet encore à la législation fédérale de couvrir largement les actes illégaux prévus par la présente Convention, mais elle admet que les Etats constitutants restent compétents pour les questions mineures ou d'intérêt purement local. Dans certains cas entrant dans cette catégorie restreinte d'actes réglementés par l'Etat constituant et non par la législation fédérale, un Etat constituant peut ne pas avoir institué une mesure qui se situerait normalement dans le champ d'application de la Convention. Ainsi, par exemple, une attaque commise contre un ordinateur personnel autonome ou un réseau d'ordinateurs connectés entre eux dans un même immeuble ne relève du pénal que si la loi de l'Etat où l'attaque a eu lieu le prévoit. En revanche, l'attaque serait une infraction fédérale en cas d'accès à l'ordinateur par l'Internet, car l'utilisation de l'Internet implique un effet sur le commerce entre Etats constitutants et avec l'étranger, condition nécessaire pour demander l'application de la législation fédérale. L'application de la présente Convention par le biais du droit fédéral des Etats-Unis ou par celui de la législation d'un autre Etat fédéral dans des circonstances analogues serait conforme aux dispositions de l'article 41.

317. Le champ d'application de la clause fédérale a été limité aux dispositions du Chapitre II (droit pénal matériel, droit procédural et compétence). Les Etats fédéraux faisant usage de cette disposition auraient encore l'obligation de coopérer avec les autres Parties sur la base du Chapitre III, même lorsque l'Etat constituant ou d'autres entités territoriales analogues dans lesquels se trouve un fugitif ou une preuve n'incrimine pas le comportement ou ne dispose pas de procédures conformément à la Convention.

318. En outre, le paragraphe 2 de l'article 41 prévoit qu'un Etat fédéral, lorsqu'il fait une réserve prévue au paragraphe 1, ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses

obligations en vertu du chapitre II. En tout état de cause, il doit se doter de moyens étendus et effectifs permettant la mise en œuvre des mesures prévues par ledit chapitre. En ce qui concerne les dispositions dont l'application relève de la compétence législative de l'Etat constituant ou d'autres entités territoriales analogues, le gouvernement fédéral porte ces dispositions à la connaissance des autorités de ces entités, avec son avis favorable en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Réserves (article 42)

319. L'article 42 prévoit un certain nombre de cas où il est possible de formuler des réserves. Cette approche tient au fait que la Convention porte sur un domaine du droit pénal et du droit de procédure pénale qui est relativement nouveau pour de nombreux Etats. En outre, la nature mondiale de la Convention, qui sera ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres, rend nécessaire de prévoir ces possibilités de réserves. Celles-ci visent à permettre au plus grand nombre d'Etats possible de devenir Parties à la Convention tout en leur permettant de conserver certaines approches et notions compatibles avec leur législation interne. En même temps, les auteurs ont cherché à limiter les possibilités de faire des réserves afin de garantir autant que faire se pouvait l'application uniforme de la Convention par les Parties. C'est pourquoi celles-ci ne peuvent faire aucune autre réserve que celles qui sont énumérées. De plus, une Partie ne peut faire une réserve qu'au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion.

320. Tenant compte du fait que, pour certaines Parties, certaines réserves étaient indispensables pour éviter une incompatibilité avec leurs principes constitutionnels ou principes juridiques fondamentaux, l'article 43 n'impose aucune délai pour le retrait des réserves. Elles doivent être retirées dès que les circonstances le permettent.

321. Afin de pouvoir exercer une certaine pression sur les Parties en vue de les amener au moins à envisager de retirer leurs réserves, la Convention autorise le Secrétaire général du Conseil de l'Europe à s'enquérir périodiquement des perspectives de retrait desdites réserves. Cette possibilité de demander des renseignements est devenue pratique courante dans le cadre de l'application de plusieurs instruments du Conseil de l'Europe. Les Parties peuvent ainsi indiquer si elles doivent maintenir leurs réserves au sujet de certaines dispositions et retirer ultérieurement celles qui sont devenues inutiles. On espère

qu'avec le temps, les Parties pourront retirer autant de réserves que possible de façon à promouvoir l'application uniforme de la Convention.

Amendements (article 44)

322. L'article 44 a pour précédent la Convention relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime (STE n° 141), où cette disposition a été insérée à titre de nouveauté en ce qui concerne les conventions de droit pénal élaborées au sein du Conseil de l'Europe. On considère que la procédure d'amendement s'applique pour l'essentiel à des modifications relativement mineures à caractère procédural ou technique. Les auteurs ont estimé que les changements importants à apporter à la Convention pourraient l'être sous la forme de Protocoles additionnels.

323. Les Parties elles-mêmes peuvent examiner la nécessité d'amendements ou de protocoles en appliquant la procédure de concertation prévue à l'article 46. Le Comité européen pour les problèmes criminels (CDPC) devra en être tenu régulièrement informé et prendre les mesures voulues pour aider les Parties à modifier ou compléter la Convention.

324. Conformément au paragraphe 5, tout amendement adopté n'entrera en vigueur qu'après que toutes les Parties auront informé le Secrétaire général qu'elles l'acceptent. Cette disposition a pour objet de ménager à la Convention la possibilité d'évoluer de façon uniforme.

Règlement des différends (article 45)

325. Le paragraphe 1 de l'article 45 dispose que le Comité européen pour les problèmes criminels doit être tenu informé de l'interprétation et de l'application des dispositions de la Convention. Le paragraphe 2 impose aux Parties l'obligation de s'efforcer de parvenir à un règlement pacifique de tout différend sur l'interprétation ou l'application de la Convention. Tout moyen de règlement du différend devra avoir été arrêté en commun par les Parties concernées. Cette disposition propose trois mécanismes possibles de règlement des différends : le recours au CDPC, à un tribunal arbitral ou à la Cour internationale de Justice.

Concertation des Parties (article 46)

326. L'article 46 institue un cadre devant permettre aux Parties de se concerter au sujet de la mise en œuvre de la Convention, des répercussions des nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique ou en relation avec l'ordinateur, et

de la collecte de preuves sous forme électronique, ainsi que de l'éventualité de compléter ou d'amender la Convention. Ces concertations devront, en particulier, examiner les questions apparues à l'occasion de l'application et de la mise en œuvre de la Convention, y compris les effets des déclarations et des réserves faites conformément aux articles 40, 41 et 42.

327. La procédure est souple : il appartient aux Parties de décider comment ou quand se rencontrer si elles le souhaitent. Les auteurs de la Convention ont jugé cette procédure utile pour permettre à toutes les Parties à la Convention, y compris les Etats non membres du Conseil de l'Europe, d'être associées – sur un pied d'égalité – à tout mécanisme de suivi, sans empiéter sur le domaine de compétence du CDPC. Celui-ci non seulement doit être tenu périodiquement au courant des consultations qui se déroulent entre les Parties, mais doit aussi les faciliter et prendre les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Compte tenu de la nécessité de prévenir les infractions relevant de la cybercriminalité et de poursuivre leurs auteurs, compte tenu aussi des questions connexes liées à la vie privée, des effets potentiels sur les activités commerciales et d'autres facteurs pertinents, il peut être utile d'associer aux concertations les parties intéressées, notamment les services de lutte contre la criminalité, les organisations non gouvernementales et le secteur privé (voir aussi le paragraphe 14).

328. Le paragraphe 3 prévoit un examen du fonctionnement de la Convention à l'issue d'un délai de trois ans à compter de son entrée en vigueur, au cours duquel des amendements pourront être proposés. Le CDPC procédera à cet examen avec l'aide des Parties.

329. Le paragraphe 4 dispose que, sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par les consultations menées conformément au paragraphe 1 de l'article 46 seront supportés par les Parties elles-mêmes. Toutefois, en sus du CDPC, le Secrétariat du Conseil de l'Europe aidera les Parties dans toutes leurs activités en rapport avec la Convention.

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination

d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189) Strasbourg, 28 janvier 2003

Les Etats membres du Conseil de l'Europe et les autres Etats parties à la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001, signataires du présent Protocole ;

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Rappelant que tous les êtres humains sont nés libres et égaux en dignité et en droits ;

Soulignant la nécessité de garantir une mise en œuvre exhaustive et efficace de tous les droits de l'homme sans distinction ni discrimination, tels qu'énoncés dans les instruments européens et autres instruments internationaux ;

Convaincus que des actes de nature raciste et xénophobe constituent une violation des droits de l'homme, ainsi qu'une menace pour l'Etat de droit et la stabilité démocratique ;

Considérant que le droit national et le droit international nécessitent de prévoir une réponse juridique adéquate à la propagande de nature raciste et xénophobe diffusée par le biais des systèmes informatiques ;

Conscients que la propagande de tels actes est souvent criminalisée par les législations nationales ;

Ayant égard à la Convention sur la cybercriminalité qui prévoit des moyens flexibles et modernes de coopération internationale, et convaincus de la nécessité d'harmoniser la lutte contre la propagande raciste et xénophobe ;

Conscients de ce que les systèmes informatiques offrent un moyen sans précédent de faciliter la liberté d'expression et de communication dans le monde entier ;

Reconnaissant que la liberté d'expression constitue l'un des principaux fondements d'une société démocratique, et qu'elle est l'une des conditions essentielles de son progrès et de l'épanouissement de chaque être humain ;

Préoccupés toutefois par le risque que ces systèmes informatiques soient utilisés à mauvais escient ou de manière abusive pour diffuser une propagande raciste et xénophobe ;

Convaincus de la nécessité d'assurer un bon équilibre entre la liberté d'expression et une lutte efficace contre les actes de nature raciste et xénophobe ;

Reconnaissant que ce Protocole ne porte pas atteinte aux principes établis dans le droit interne concernant la liberté d'expression ;

Tenant compte des instruments juridiques internationaux pertinents dans ce domaine, et en particulier de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales et de son Protocole n° 12 relatif à l'interdiction générale de la discrimination, des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, en particulier de la Convention sur la cybercriminalité et de la Convention internationale des Nations Unies du 21 décembre 1965 sur l'élimination de toutes les formes de discrimination raciale, l'Action commune du 15 juillet 1996 de l'Union européenne adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne concernant l'action contre le racisme et la xénophobie ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la cybercriminalité, ainsi que celle contre le racisme et la xénophobie ;

Prenant également en compte le Plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2^e Sommet, tenu à Strasbourg les 10 et 11 octobre 1997, afin de chercher des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit :

Chapitre I – Dispositions communes

Article 1 – But

Le but du présent Protocole est de compléter, pour les Parties au Protocole, les dispositions de la Convention sur la cybercriminalité, ouverte à la signature à Budapest le 23 novembre 2001 (appelé ci-après « la Convention ») eu égard à l'incrimination des actes de nature raciste et xénophobe diffusés par le biais de systèmes informatiques.

Article 2 – Définition

1. Aux fins du présent Protocole, l'expression :

« *matériel raciste et xénophobe* » désigne tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes.

2. Les expressions et termes employés dans ce Protocole sont interprétés de la même manière qu'ils le sont dans la Convention.

Chapitre II – Mesures à prendre au niveau national

Article 3 – Diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants :

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel raciste et xénophobe.

2. Une Partie peut se réserver le droit de ne pas imposer de responsabilité pénale aux conduites prévues au paragraphe 1 du présent article lorsque le matériel, tel que défini à l'article 2, paragraphe 1, préconise, encourage ou incite à une discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles.

3. Sans préjudice du paragraphe 2 du présent article, une Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 aux cas de discrimination

pour lesquels elle ne peut pas prévoir, à la lumière des principes établis dans son ordre juridique interne concernant la liberté d'expression, les recours efficaces prévus au paragraphe 2.

Article 4 – Menace avec une motivation raciste et xénophobe

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant :

la menace, par le biais d'un système informatique, de commettre une infraction pénale grave, telle que définie par le droit national, envers (i) une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) un groupe de personnes qui se distingue par une de ces caractéristiques.

Article 5 – Insulte avec une motivation raciste et xénophobe

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, dans son droit interne, lorsqu'il est commis intentionnellement et sans droit, le comportement suivant :

l'insulte en public, par le biais d'un système informatique, (i) d'une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou (ii) d'un groupe de personnes qui se distingue par une de ces caractéristiques.

- a. soit exiger que l'infraction prévue au paragraphe 1 du présent article ait pour effet d'exposer la personne ou le groupe de personnes visées au paragraphe 1 à la haine, au mépris ou au ridicule ;
- b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 6 – Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité

1. Chaque Partie adopte les mesures législatives qui se révèlent nécessaires pour ériger en infractions pénales, dans son droit interne, lorsqu'ils sont commis intentionnellement et sans droit, les comportements suivants :

la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international, établi par l'accord de Londres du 8 août 1945, ou par tout autre tribunal international établi par des instruments internationaux pertinents et dont la juridiction a été reconnue par cette Partie.

2. Une Partie peut :

- a. soit prévoir que la négation ou la minimisation grossière, prévues au paragraphe 1 du présent article, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ;
- b. soit se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 1 du présent article.

Article 7 – Aide et complicité

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, en vertu de son droit interne, lorsqu'il est commis intentionnellement et sans droit, le fait d'aider à perpétrer une infraction telle que définie dans ce Protocole, ou d'en être complice, avec l'intention qu'une telle infraction soit commise.

Chapitre III – Relations entre la Convention et ce Protocole

Article 8 – Relations entre la Convention et ce Protocole

- 1. Les articles 1, 12, 13, 22, 41, 44, 45 et 46 de la Convention s'appliquent, *mutatis mutandis*, à ce Protocole.
- 2. Les Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole.

Chapitre IV – Dispositions finales

Article 9 – Expression du consentement à être lié

1. Le présent Protocole est ouvert à la signature des Etats signataires de la Convention, qui peuvent exprimer leur consentement à être liés par :
 - a. la signature sans réserve de ratification, d'acceptation ou d'approbation ;
ou
 - b. la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.
2. Un Etat ne peut signer le présent Protocole sans réserve de ratification, d'acceptation ou d'approbation ni déposer un instrument de ratification, d'acceptation ou d'approbation s'il n'a pas déjà déposé ou ne dépose pas simultanément un instrument de ratification, d'acceptation ou d'approbation de la Convention.
3. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

Article 10 – Entrée en vigueur

1. Le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats auront exprimé leur consentement à être liés par le Protocole conformément aux dispositions de l'article 9.
2. Pour tout Etat qui exprimera ultérieurement son consentement à être lié par le Protocole, celui-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de sa signature sans réserve de ratification, d'acceptation ou d'approbation ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

Article 11 – Adhésion

1. Après l'entrée en vigueur du présent Protocole, tout Etat qui a adhéré à la Convention pourra adhérer également au Protocole.
2. L'adhésion s'effectuera par le dépôt, près le Secrétaire Général du Conseil de l'Europe, d'un instrument d'adhésion qui prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de son dépôt.

Article 12 – Réserves et déclarations

1. Les réserves et les déclarations formulées par une Partie concernant une disposition de la Convention s'appliqueront également à ce Protocole, à moins que cette Partie n'exprime l'intention contraire au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion.

2. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou des réserves prévues aux articles 3, 5 et 6 du présent Protocole. Une Partie peut aussi formuler, par rapport aux dispositions de ce Protocole, les réserves prévues à l'article 22, paragraphe 2, et à l'article 41, paragraphe 1, de la Convention, sans préjudice de la mise en œuvre faite par cette Partie par rapport à la Convention. Aucune autre réserve ne peut être formulée.

3. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la possibilité de prévoir des éléments additionnels, tels que prévus à l'article 5, paragraphe 2.a, et à l'article 6, paragraphe 2.a, de ce Protocole.

Article 13 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'article 12 ci-dessus retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification de retrait par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 12 des informations sur les perspectives de leur retrait.

Article 14 – Application territoriale

1. Toute Partie peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera le présent Protocole.

2. Toute Partie peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de ce Protocole à tout autre territoire désigné dans la déclaration. Le Protocole entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3. Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 15 – Dénonciation

1. Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.

2. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 16 – Notification

Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant participé à l'élaboration du présent Protocole, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

- a. toute signature ;
- b. le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;
- c. toute date d'entrée en vigueur du présent Protocole conformément à ses articles 9, 10 et 11 ;
- d. tout autre acte, notification ou communication ayant trait au présent Protocole.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé le présent Protocole.

Fait à Strasbourg, le 28 janvier 2003, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres ayant participé à l'élaboration du présent Protocole et à tout Etat invité à y adhérer.

Rapport explicatif du Premier Protocole additionnel

Le texte de ce Rapport explicatif ne constitue pas un instrument d'interprétation authentique du texte du Protocole, bien qu'il puisse faciliter la compréhension des dispositions qui y sont contenues. Le Protocole a été ouvert à la signature à Strasbourg, le 28 janvier 2003, à l'occasion de la Première Partie de la session 2003 de l'Assemblée parlementaire.

Introduction

1. Depuis l'adoption de la Déclaration universelle des droits de l'homme en 1948 la communauté internationale a réalisé des progrès importants dans la lutte contre le racisme, la discrimination raciale, la xénophobie et l'intolérance qui y est associée. Des règles ont été adoptées aux niveaux national et international et un certain nombre d'instruments internationaux de protection des droits de l'homme a été mis en place, notamment la Convention internationale de New York de 1965 sur l'élimination de toute forme de discrimination raciale (CERD) qui a été élaborée dans le cadre des Nations Unies. En dépit de ces progrès, le rêve d'un monde sans haine ni discrimination raciale ne s'est que partiellement concrétisé.
2. Alors que les développements technologiques, économiques et commerciaux rapprochent les peuples du monde entier, la discrimination raciale, la xénophobie et d'autres formes d'intolérance continuent d'exister dans nos sociétés. La mondialisation présente des risques pouvant conduire à l'exclusion et à l'accroissement des inégalités, très souvent sur une base raciale et ethnique.
3. En particulier, l'apparition de réseaux de communication globale comme Internet offre à certaines personnes des moyens modernes et puissants pour soutenir le racisme et la xénophobie et pour diffuser facilement et largement des contenus exprimant de telles idées. Pour pouvoir mener des enquêtes et poursuivre ces personnes, la coopération internationale est essentielle. La Convention sur la cybercriminalité (STE 185), appelée ci-après «la Convention», a été élaborée pour permettre une entraide concernant les crimes informatiques au sens large du terme, conçue de manière souple et moderne. Ce Protocole poursuit deux objectifs : premièrement, harmoniser le droit pénal matériel dans la lutte contre le racisme et la xénophobie sur l'Internet et deuxièmement, améliorer la coopération internationale dans ce domaine. Une harmonisation de ce type facilite la lutte contre cette criminalité

aux niveaux national et international. Prévoir des infractions correspondantes dans le droit interne peut prévenir l'abus des systèmes informatiques à des fins racistes dans des Parties qui n'ont pas une législation très bien définie dans ce domaine. La coopération internationale (en particulier l'extradition et l'entraide judiciaire) se trouve facilitée, par exemple en ce qui concerne la règle de la double incrimination.

4. Le comité chargé de rédiger la Convention a examiné la possibilité d'inclure des infractions liées au contenu autres que la pornographie enfantine, comme la diffusion de propagande raciste par le biais de systèmes informatiques. Toutefois, le comité n'a pas pu parvenir à un consensus concernant l'incrimination d'un tel comportement. Alors que beaucoup de délégations se sont déclarées favorables à l'idée d'en faire une infraction pénale, plusieurs se sont dites très préoccupées par cette démarche qui porterait atteinte à la liberté d'expression. En raison de la complexité de cette question, il a été décidé que le comité saisirait le Comité européen pour les problèmes criminels (CDPC) de la question de la rédaction d'un protocole additionnel à la Convention.

5. L'Assemblée parlementaire, dans son Avis n° 226(2001), a recommandé la rédaction sur le champ d'un protocole additionnel à la future Convention, intitulé «élargissement du champ d'application de la Convention à de nouvelles formes d'infractions», qui définisse et incrimine notamment la diffusion de propagande raciste.

6. Le Comité des Ministres a donc confié au Comité européen pour les problèmes criminels (CDPC), et notamment à son Comité d'experts sur l'incrimination des actes de nature raciste et xénophobe par le biais de systèmes informatiques (PC-RX), le soin de rédiger un projet de protocole additionnel, instrument juridique obligatoire ouvert à la signature et à la ratification des Parties contractantes à la Convention, pour traiter en particulier des questions suivantes :

- i. la définition et l'étendue d'éléments en vue de l'incrimination des actes de nature raciste et xénophobe commis à travers les réseaux informatiques, y compris la production, l'offre, la diffusion ou d'autres formes de dissémination de matériels ou de messages avec un tel contenu, à travers les réseaux informatiques ;
- ii. la mesure dans laquelle les dispositions de droit matériel, procédural et de coopération internationale contenues dans la

Convention sur la cybercriminalité s'appliquent aux enquêtes et aux poursuites relatives aux infractions à établir dans le Protocole additionnel.

7. Ce protocole comporte un élargissement de la portée de la Convention, y compris de ses dispositions sur le fond, la procédure et la coopération internationale, de manière à couvrir également les infractions concernant la propagande raciste et xénophobe. Ainsi, outre l'harmonisation des éléments de droit matériel concernant ces comportements, le Protocole vise à améliorer la possibilité qu'ont les Parties d'utiliser dans ce domaine les moyens de coopération internationale prévus par la Convention.

Commentaires concernant les articles du protocole

Chapitre I – Dispositions communes

Article 1 – Objet

8. Le but du présent Protocole est de compléter, pour les Parties au Protocole les dispositions de la Convention par l'incrimination des actes de nature raciste et xénophobe commis par le biais des systèmes informatiques.

9. Les dispositions du Protocole ont un caractère obligatoire. Pour satisfaire à ces obligations, les Etats parties doivent non seulement promulguer une législation appropriée, mais aussi veiller à ce qu'elle soit correctement mise en œuvre.

Article 2 – Définition

Paragraphe 1 – « Matériel raciste et xénophobe »

10. De nombreux instruments juridiques ont été élaborés aux niveaux international et national pour lutter contre le racisme ou la xénophobie. Les rédacteurs de ce Protocole ont notamment pris en compte i. la Convention internationale sur l'élimination de toutes les formes de discrimination raciale ; ii. le Protocole n° 12 (STE 177) à la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH) ; iii. l'action commune du 15 juillet 1996 de l'Union européenne adoptée par le Conseil sur la base de l'article K.3 du Traité sur l'Union européenne, concernant des actions pour combattre le racisme et la xénophobie ; iv. la Conférence mondiale contre le racisme, la discrimination raciale, la xénophobie et l'intolérance qui y est associée (Durban, 30 août-8 septembre 2001) ; v. les conclusions de la Conférence européenne contre le racisme (Strasbourg, 13 octobre 2000) ;

vi. l'étude complète publiée en août 2000 par la Commission européenne contre le racisme et l'intolérance (ECRI) (ECRI(2000)27) et vii. la proposition de la Commission européenne de novembre 2001 pour une décision-cadre du Conseil de l'Union européenne sur la lutte contre le racisme et la xénophobie.

11. L'article 10 de la CEDH reconnaît le droit à la liberté d'expression, qui inclut la liberté d'avoir une opinion et de recevoir et de transmettre des informations et des idées. Comme l'a précisé la Cour dans sa jurisprudence « l'article 10 de la CEDH vaut non seulement pour les « informations » ou « idées » accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi pour celles qui heurtent, choquent ou inquiètent l'Etat ou une fraction quelconque de la population¹² ». Toutefois, la Cour a établi que les actions des Etats visant à restreindre le droit à la liberté d'expression étaient justifiées au regard du paragraphe 2 de l'article 10 de la CEDH, notamment lorsque ces idées et ces expressions portent atteinte aux droits des tiers. Ce Protocole, sur la base des instruments nationaux et internationaux, établit dans quelle mesure la diffusion d'expressions et d'idées racistes et xénophobes porte atteinte aux droits des individus.

12. La définition contenue à l'article 2 fait référence au matériel écrit (par exemple, textes, livres, magazines, déclarations, messages, etc.), aux images (par exemple, illustrations, photos, dessins, etc.) ou à toute autre représentation d'idées ou de théories, de nature raciste et xénophobe, dans un format tel qu'il puisse être conservé, traité et transmis par le biais d'un système informatique.

13. La définition contenue à l'article 2 de ce Protocole se réfère à un comportement auquel le contenu du matériel peut mener, plutôt qu'à l'expression de sentiments/de convictions/d'aversions contenue dans le matériel en question. La définition est fondée, dans la mesure du possible, sur les définitions et les documents nationaux et internationaux existants (NU, UE).

14. Ce matériel doit préconiser et encourager la haine, la discrimination ou la violence ou inciter à de tels actes. « Préconiser » se réfère à un plaidoyer en faveur de la haine, de la discrimination ou de la violence, « encourager » se réfère à promouvoir ou aider la haine, la discrimination ou la violence et « inciter » se réfère à presser d'autres à agir avec haine, discrimination ou violence.

15. L'expression « violence » se réfère à l'usage illégal de la force, alors que le mot « haine » correspond à une extrême aversion ou volonté d'offenser.

12. Voir dans ce contexte, par exemple, l'arrêt de l'affaire Handyside du 7 décembre 1976, série A, n° 24, page 23, paragraphe 49.

16. En interprétant le terme « discrimination », la CEDH (article 14 et Protocole n° 12) et la jurisprudence pertinente, ainsi que l'article 1 du CERD (qui contient des détails sur la notion de « discrimination raciale »), devraient être gardés à l'esprit. L'interdiction de discriminer contenue dans la CEDH garantit à toute personne relevant de la juridiction d'un Etat Partie l'égalité dans l'exercice des droits et libertés contenus dans la CEDH. L'article 14 de la CEDH établit une obligation générale pour les Etats d'interdire la discrimination, accessoire aux droits et libertés qui sont garantis par la CEDH. Dans ce contexte, la « discrimination » évoque un traitement différent injustifié réservé à des personnes ou à un groupe de personnes en fonction de certaines caractéristiques. Dans plusieurs arrêts (par exemple, l'arrêt Linguistique belge, l'arrêt Abdulaziz, Cabales et Balkandali¹³), la Cour européenne des Droits de l'Homme déclare : « une distinction est discriminatoire si elle « manque de justification objective et raisonnable », c'est-à-dire si elle ne poursuit pas un « but légitime » ou s'il n'y a pas de « rapport raisonnable de proportionnalité entre les moyens employés et le but visé » » (arrêt du 28 mai 1985, série A, n° 94, paragraphe 72). Le point de savoir si un traitement est ou non discriminatoire doit être examiné à la lumière des circonstances particulières. En ce qui concerne plus particulièrement la discrimination raciale, une indication pour l'interprétation de ce terme peut être trouvée à l'article 1 du CERD qui établit que « discrimination raciale » vise « toute distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, qui a pour but ou pour effet de détruire ou de compromettre la reconnaissance, la jouissance ou l'exercice, dans des conditions d'égalité, des droits de l'homme et des libertés fondamentales dans les domaines politique, économique, social et culturel ou dans tout autre domaine de la vie publique ».

17. La haine, la discrimination ou la violence peuvent être dirigés contre une personne ou un groupe de personnes, en raison de leur appartenance à un groupe caractérisé par « race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments ».

18. Ces motifs ne sont pas exactement identiques à ceux énumérés à l'article 1 du Protocole n° 12 à la CEDH, par exemple, car certains des motifs contenus dans cet article sont étrangers au concept de racisme ou de xénophobie, ni à ceux énoncés dans la Convention internationale sur l'élimination de toutes les

13. Abulaziz, Cabales et Balkandali, arrêt du 28 mai 1985, Série A n° 94, p. 32, para. 62 ; Arrêt linguistique belge, arrêt du 23 juillet 1968, Série A n° 6, p. 34, para. 10.

formes de discrimination raciale, qui traite de la « discrimination raciale » en général et non du « racisme » en tant que tel. En général, ces motifs doivent être interprétés selon le droit et la pratique nationaux et internationaux. Toutefois, certains d'entre eux requièrent des explications supplémentaires quant à leur signification spécifique dans le contexte de ce Protocole.

19. « L'ascendance » se réfère essentiellement aux personnes ou groupes de personnes dont certains ascendants pouvaient être identifiées par des caractéristiques (telles que la race ou la couleur). Toutefois, même si ces caractéristiques n'existent pas nécessairement à l'heure actuelle, en raison de leur ascendance, ces personnes ou groupes de personnes peuvent encore être sujet à la haine, à la discrimination ou à la violence. « L'ascendance » ne se réfère pas à l'origine sociale.

20. La notion « d'origine nationale », doit être interprétée dans un large sens factuel. Il peut se référer à l'histoire d'une personne, non seulement quant à la nationalité ou l'origine de ses ancêtres, mais aussi par rapport à sa propre appartenance nationale, indépendamment du fait que cette personne possède ou non cette nationalité au sens juridique du terme. Lorsqu'une personne possède plusieurs nationalités ou est apatride, l'interprétation large de cette notion permet de la protéger si elle est discriminée sur la base de l'un de ces motifs. De plus, la notion « d'origine nationale » peut non seulement se référer à l'appartenance à un Pays qui est reconnu comme tel par la communauté internationale, mais aussi aux minorités ou à tout autre groupe de personne avec des caractéristiques similaires.

21. La notion de « religion » se trouve souvent dans les instruments internationaux et dans la législation nationale. Ce terme se réfère à des convictions et à des croyances. Inclure ce terme en tant que tel dans la définition pourrait entraîner le risque de dépasser le champ d'application du Protocole. Toutefois, la religion peut être utilisée comme prétexte, alibi ou substitut aux autres facteurs énumérés dans la définition. Le terme « religion » doit donc être interprétée dans ce sens limité.

Paragraphe 2

22. En veillant à ce que les termes et les expressions utilisés dans le Protocole soient interprétés conformément à la Convention, cet article garantit une interprétation uniforme des deux textes. Ceci veut dire que les termes et les expressions employés dans ce Rapport explicatif sont interprétés de la même manière que dans le Rapport explicatif de la Convention.

Chapitre II – Mesures à prendre au niveau national

Considérations générales

23. Les infractions telles que définies dans ce Protocole contiennent un certain nombre d'éléments communs qui ont été repris de la Convention. Pour plus de clarté, les paragraphes correspondants du Rapport Explicatif de la Convention ont été reproduits ci-après.

24. Une caractéristique des infractions en question est que leurs auteurs doivent expressément avoir agi « sans droit ». Cette expression rend compte du fait que le comportement décrit n'est pas toujours punissable en soi, mais peut être légal ou justifié non seulement par des exceptions légales classiques (consentement, légitime défense ou nécessité), mais dans les cas où d'autres principes ou intérêts excluent toute responsabilité pénale (par exemple à des fins de maintien de l'ordre, de recherche ou académiques). L'expression « sans droit » tire son sens du contexte dans lequel elle est utilisée. Ainsi, sans restreindre la marge de manœuvre qu'ont les Parties pour interpréter ce concept dans leur droit interne, cette expression peut renvoyer à un comportement qui ne repose sur aucune compétence (législative, exécutive, administrative, judiciaire, contractuelle ou consensuelle) ou à un comportement qui n'est couvert ni par des exceptions légales, excuses et faits justificatifs établis, ni par des principes de droit interne pertinents. Le Protocole ne concerne pas, par conséquent, les comportements conformes aux compétences gouvernementales légales (par exemple, lorsque le gouvernement de la Partie concernée agit dans un but de maintien de l'ordre public, de protection de la sécurité nationale ou dans le cadre d'une instruction pénale). De plus, les activités légitimes et ordinaires inhérentes à la conception des réseaux ainsi que les pratiques d'exploitation ou de commerce légitimes ou ordinaires ne devraient pas être érigées en infractions pénales. Il appartient aux Parties de déterminer les modalités d'application desdites exceptions dans leur ordre juridique interne (en droit pénal ou autre).

25. Toutes les infractions énumérées dans le Protocole doivent être commises de façon « intentionnelle » pour que la responsabilité pénale soit engagée. Dans certains cas, un élément intentionnel spécifique supplémentaire fait partie intégrante de l'infraction. Les auteurs du Protocole, comme ceux de la Convention, se sont entendus pour considérer que l'interprétation du mot « intentionnellement » doit être laissée aux droits internes. Une personne ne peut être responsable pour une quelconque infraction contenue dans ce Protocole si elle n'a pas agi avec intention délictueuse. Il ne suffit pas, par exemple, pour

que la responsabilité pénale d'un fournisseur de services soit engagée, que ce dernier sert d'intermédiaire pour la transmission de ce type de matériel par le biais d'un site Web ou d'un bavardoir, en l'absence de l'intention requise en droit interne dans le cas particulier. De plus, un fournisseur de service n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale.

26. En ce qui concerne la définition de «système informatique», elle est identique à celle contenue dans la Convention et expliquée dans son Rapport explicatif.

Article 3 – Diffusion de matériel raciste et xénophobe dans les systèmes informatiques

27. Cet article exige des Etats Parties d'incriminer la diffusion ou les autres formes de mise à disposition du public de matériel raciste et xénophobe par le biais d'un système informatique.

28. Par «diffusion», il faut entendre l'action consistant à disséminer du matériel raciste et xénophobe à autrui, tandis que la «mise à disposition» désigne l'action consistant à mettre du matériel raciste et xénophobe en ligne pour qu'il soit utilisé par autrui. Cette expression englobe par ailleurs la création ou la compilation d'hyperliens visant à faciliter l'accès à ce matériel.

29. Le terme «au/du public» utilisé à l'article 3 indique clairement que toute conversation ou expression privée communiquée ou transmise par le biais d'un système informatique ne rentre pas dans le champ d'application de cette disposition. En effet, de telles communications ou expressions, comme d'autres formes traditionnelles de correspondance, sont protégées par l'article 8 de la CEDH.

30. La question de déterminer si une communication de matériel raciste et xénophobe doit être considérée comme une communication privée ou une diffusion au public, doit être examinée à la lumière de circonstances spécifiques. En premier lieu, ce qui importe est la volonté de l'émetteur du message de le transmettre à une personne déterminée. La présence de cette intention subjective peut être établie sur la base d'un certain nombre de facteurs objectifs, tels que le contenu du message, la technologie employée, les mesures de sécurité appliquées, le contexte dans lequel celui-ci est émis. Lorsque ces messages sont envoyés à plusieurs récepteurs à la fois, le nombre de récepteurs et la nature de la relation entre l'émetteur et le récepteur sont des facteurs pertinents pour déterminer si une telle communication peut encore être considérée comme privée.

31. Echanger du matériel raciste et xénophobe dans un *chat-room*, le distribuer dans des newsgroups ou des forums de discussion, sont des exemples de mise à disposition du public d'un tel matériel. Dans ce cas, le matériel est accessible à toute personne. Même lorsque l'accès à ce matériel exigerait une autorisation par le biais d'un mot de passe, le matériel en question serait accessible au public lorsque cette autorisation est donnée à tout le monde ou à toute personne qui présente certains critères. Afin de déterminer si la mise à disposition ou la diffusion était ou non au public, la nature de la relation entre les personnes concernées devrait être prise en considération.

32. Les paragraphes 2 et 3 visent à prévoir une possibilité de réserve dans des cas tout à fait limités. Ces paragraphes devraient être lus ensemble et en séquence. Une Partie a, premièrement, la possibilité de ne pas imposer de responsabilité pénale aux comportements prévus dans cet article, lorsque le matériel préconise, encourage ou incite à la discrimination qui n'est pas associée à la haine ou à la violence, à condition que d'autres recours efficaces soient disponibles. Par exemple, ces recours peuvent être de nature civile ou administrative. Lorsqu'une Partie ne peut pas, à cause de principes établis dans son système juridique interne concernant la liberté d'expression, prévoir de tels recours, elle peut se réserver le droit de ne pas appliquer l'obligation contenue au paragraphe 1 de cet article, si elle concerne seulement le fait de préconiser, encourager ou inciter à une discrimination qui n'est pas associée à la haine ou à la violence. Une Partie peut aussi restreindre encore le champ d'application de cette réserve en prévoyant que la discrimination vise, par exemple, à insulter, dégrader ou menacer un groupe de personnes.

Article 4 – Menace avec une motivation raciste et xénophobe

33. La plupart des législations prévoient déjà l'incrimination de la menace en général. Les rédacteurs sont convenus de souligner dans le Protocole que, sans aucun doute, la menace avec une motivation raciste et xénophobe doit être pénalement sanctionnée.

34. La notion de « menace » peut se référer à une intimidation qui provoque la crainte chez la personne envers laquelle la menace est dirigée, qu'elle risque d'être victime d'une infraction pénale grave (par exemple, qui porte atteinte à la vie, à l'intégrité physique ou personnelle, aux biens, etc., de la victime ou de sa famille). Les Etats déterminent librement ce qui constitue une infraction pénale grave.

35. Selon cette disposition, la menace doit s'adresser soit (i) à une personne au motif qu'elle appartient à un groupe caractérisé par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, soit (ii) à un groupe de personnes défini par l'une de ces caractéristiques. La menace ne doit pas être nécessairement faite en public. En effet, cet article couvre aussi la menace privée.

Article 5 – Insulte avec une motivation raciste et xénophobe

36. L'article 5 traite de l'insulte en public, d'une personne ou d'un groupe au motif qu'ils appartiennent ou sont considérés comme appartenant à un groupe avec certaines caractéristiques. La notion « d'insulte » se réfère à toute expression outrageante, terme de mépris ou invective qui porte atteinte à l'honneur ou à la dignité de la personne. Il devrait clairement résulter de l'expression elle-même que l'insulte directement liée à l'appartenance à un groupe de la personne insultée. Contrairement au cas de la menace, l'insulte exprimée lors d'une communication privée n'est pas couverte par cette disposition.

37. Le paragraphe 2(i) permet aux Parties de prévoir que la conduite doit aussi avoir pour effet d'exposer, non seulement en théorie, mais aussi en pratique, la personne ou le groupe de personnes en question à la haine, au mépris ou au ridicule.

38. Le paragraphe 2(ii) permet aux Parties de formuler une réserve qui va encore plus loin, jusqu'à exclure l'application du paragraphe 1.

Article 6 – Négation, minimisation grossière, approbation ou justification du génocide ou des crimes contre l'humanité

39. Ces dernières années, diverses affaires ont été traitées par des tribunaux nationaux où des personnes (dans le public, dans les médias, etc.) ont élaboré des idées ou des théories visant à minimiser, nier ou justifier les crimes graves commis au cours de la seconde guerre mondiale (en particulier l'Holocauste). La motivation de tels comportements est souvent présentée sous le prétexte de la recherche scientifique, alors qu'en réalité, le but exact est de soutenir et d'encourager la motivation politique qui avait donné lieu à l'Holocauste. De plus, ces comportements ont aussi inspiré ou même stimulé et développé les activités illégales de groupes racistes et xénophobes, y compris par le biais de systèmes informatiques. L'expression de ces idées insulte (la mémoire de)

toute personne qui a été victime de l'Holocauste, ainsi que leur famille. Elle porte en outre atteinte à la dignité de la communauté humaine.

40. L'article 6 du Protocole, qui a une structure similaire à celle de l'article 3, traite ce problème. Les rédacteurs s'entendent qu'il est important d'incriminer toute expression qui nie, minimise de manière grossière, approuve ou justifie des actes constitutifs de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international établi par l'accord de Londres du 8 avril 1945. Ceci à cause du fait que les actes qui ont donné lieu à des génocides et à des crimes contre l'humanité, se sont déroulés entre 1940 et 1945. Toutefois, les rédacteurs ont relevé que, depuis lors, d'autres cas de génocide et de crimes contre l'humanité, qui étaient motivés par des idées et des théories de nature raciste et xénophobe, ont été perpétrés. Les rédacteurs ont dès lors considéré qu'il était nécessaire de ne pas limiter le champ d'application de cette disposition aux seuls crimes commis par le régime nazi pendant la seconde guerre mondiale, et établis comme tels par le Tribunal de Nürnberg, mais de l'étendre aussi aux génocides et crimes contre l'humanité constatés par d'autres tribunaux internationaux établis après 1945 par des instruments internationaux pertinents (par exemple, des Résolutions du Conseil de Sécurité des Nations Unies, des traités multilatéraux, etc.). De tels tribunaux pourraient être, par exemple, les Tribunaux pénaux pour l'ex-Yougoslavie, pour le Rwanda, la Cour Pénale Internationale. Cet article permet de se référer à des décisions finales et obligatoires de tribunaux internationaux futurs, dans la mesure où la juridiction de tels tribunaux est reconnue par la Partie à ce Protocole.

41. Cette disposition vise à poser clairement le principe que des faits, dont la vérité historique a été judiciairement établie, ne peuvent pas être niés, minimisés de manière grossière, approuvés ou justifiés pour soutenir ces théories et ces idées détestables.

42. La Cour européenne des Droits de l'Homme a d'ailleurs indiqué clairement que la négation ou la révision de « faits historiques clairement établis – tel que l'Holocauste – [...] se verrait soustraite par l'article 17 à la protection de l'article 10 » de la CEDH (voir à cet égard l'arrêt *Lehideux et Isorni* du 23 septembre 1998¹⁴).

43. Le paragraphe 2 de l'article 6 donne la faculté aux Parties (i) soit d'exiger, à travers une déclaration, que la négation ou la minimisation grossière

14. *Lehideux et Isorni* arrêt du 23 septembre 1998, publié dans les Rapports 1998-VII, paragraphe 47.

mentionnées au paragraphe 1 de l'article 6, soient commises avec l'intention d'inciter à la haine, à la discrimination ou à la violence contre une personne ou un groupe de personnes, en raison de la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, (ii) soit de formuler une réserve, qui leur permettrait de ne pas appliquer, en tout ou en partie, cette disposition.

Article 7 – Aide et complicité

44. Cet article vise à ériger en infraction pénale tout acte de complicité en vue de la perpétration d'une des infractions établies en vertu des articles 3 à 6 du Protocole. Contrairement à la Convention, le Protocole n'incrimine pas la tentative de commission des infractions contenues dans le Protocole, car la plupart des conduites qui y sont criminalisées ont une nature préparatoire.

45. La responsabilité est engagée en cas de complicité lorsque la personne qui commet une infraction établie par le Protocole est aidée par une autre personne qui a également l'intention que l'infraction soit commise. Ainsi, par exemple, bien que la transmission par le biais de l'Internet de matériel raciste et xénophobe requière l'assistance de fournisseurs de services agissant comme intermédiaires, un fournisseur de services qui n'a pas d'intention criminelle ne peut être tenu responsable au titre de cette section. Les fournisseurs de services ne sont donc pas tenus de surveiller activement le contenu pour éviter la responsabilité pénale en application de cette disposition.

46. Comme pour toutes les infractions établies en vertu du Protocole, l'acte de complicité doit être commis intentionnellement.

Chapitre III – Relations entre la Convention et ce Protocole

Article 8 – Relations entre la Convention et ce Protocole

47. L'article 8 concerne les relations entre la Convention et ce Protocole. Il évite d'inclure un certain nombre de dispositions de la Convention dans le Protocole. Il indique que certaines des dispositions de celle-ci s'appliquent, *mutatis mutandis*, à ce Protocole (par exemple, celles qui concernent la responsabilité et les sanctions, la compétence et une partie des dispositions finales). Le paragraphe 2 de l'article 8 rappelle aux Parties que les mesures définies dans la Convention devraient être appliquées aux infractions prévues par ce Protocole. Pour plus de clarté, les articles pertinents ont été précisés.

Chapitre IV – Dispositions finales

48. Les dispositions contenues dans ce chapitre sont, pour l'essentiel, tirées du « Modèle de clauses finales des conventions et accords conclus au sein du Conseil de l'Europe » approuvé par le Comité des Ministres du Conseil de l'Europe lors de la 315^e réunion des Délégués des Ministres en février 1980. Etant donné que la majorité des articles 9 à 16 utilise le vocabulaire normalisé du modèle de clauses ou est fondée sur la longue pratique du Conseil de l'Europe en matière de traités, ces articles n'appellent aucun commentaire particulier. Toutefois, certaines modifications des clauses types ou certaines clauses nouvelles requièrent une explication. On notera à cet égard que les clauses types ont été adoptées en tant qu'ensemble non contraignant de dispositions. Comme indiqué dans l'introduction aux clauses types, « les présentes clauses finales types ne visent qu'à faciliter la tâche des comités d'experts et éviter des différences de libellé qui n'auraient aucune justification réelle. Les clauses types ne sont nullement contraignantes : des clauses différentes peuvent être adaptées à des situations différentes » (voir aussi dans ce contexte les paragraphes 304-330 du rapport explicatif de la Convention).

49. Le paragraphe 2 de l'article 12 spécifie que les Parties peuvent utiliser les réserves telles que définies aux articles 3, 5 et 6 de ce Protocole. Aucune autre réserve ne peut être formulée.

50. Ce Protocole est ouvert à la seule signature des signataires de la Convention. Il entrera en vigueur trois mois après sa ratification par cinq Parties à la Convention qui ont exprimés leur consentement pour être liées au Protocole (articles 9-10).

51. La Convention permet des réserves concernant certaines de ces dispositions qui, à travers la clause de connexion de l'article 8 du Protocole, peuvent aussi avoir un effet sur les obligations d'une Partie au titre de ce Protocole. Toutefois, une Partie peut notifier le Secrétaire Général qu'elle n'appliquera pas une réserve à ce Protocole. Ceci est expressément prévu par l'article 12 paragraphe 2 du Protocole.

52. Cependant, lorsqu'une Partie n'a pas utilisé une réserve ou une déclaration au titre de la Convention, elle peut avoir besoin de restreindre ses obligations par rapport aux infractions contenues dans ce Protocole. Le paragraphe 2 de l'article 12 permet aux Parties de le faire, concernant l'article 22, paragraphe 2, et l'article 41, paragraphe 1, de la Convention.

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (CETS n° 224) Strasbourg, 12 mai 2022¹⁵

Préambule

Les États membres du Conseil de l'Europe et les autres États Parties à la Convention sur la cybercriminalité (STE n° 185; ci-après «la Convention»), ouverte à la signature à Budapest le 23 novembre 2001, signataires du présent Protocole,

Gardant à l'esprit la portée et l'impact de la Convention dans le monde entier;

Rappelant que la Convention est déjà complétée par le Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189), ouvert à la signature à Strasbourg le 28 janvier 2003 (ci-après le «Premier Protocole»), pour ce qui est des Parties audit Protocole;

Prenant en compte les traités existants du Conseil de l'Europe relatifs à la coopération en matière pénale ainsi que d'autres accords et arrangements relatifs à la coopération en matière pénale conclus entre les Parties à la Convention;

15. Texte corrigé conformément à la décision du Comité des Ministres (1479^e réunion des Délégués des Ministres, 31 octobre 2023).

Compte tenu également de 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 son Protocole d'amendement (STCE n° 223), ouvert à la signature à Strasbourg le 10 octobre 2018, et auquel tout État peut être invité à adhérer ;

Reconnaissant l'utilisation croissante des technologies de l'information et de la communication, y compris des services internet, et l'augmentation de la cybercriminalité, qui constitue une menace pour la démocratie et l'État de droit, et que de nombreux États considèrent également comme une menace pour les droits de l'homme ;

Reconnaissant également le nombre croissant de victimes de la cybercriminalité et l'importance d'obtenir justice pour ces victimes ;

Rappelant que les gouvernements ont le devoir de protéger la société et les personnes contre le crime commis non seulement dans le monde réel mais aussi dans le monde virtuel, notamment en diligentant des enquêtes et des poursuites pénales efficaces ;

Conscients que les preuves recueillies de toute infraction pénale sont de plus en plus stockées sous forme électronique sur des systèmes informatiques situés dans des juridictions étrangères, multiples ou inconnues, et convaincus que des mesures complémentaires sont nécessaires pour obtenir légalement ces preuves afin de permettre une réponse efficace par la justice pénale et de défendre l'État de droit ;

Reconnaissant la nécessité d'une coopération accrue et plus efficace entre les États et le secteur privé et que, dans ce contexte, une plus grande clarté ou sécurité juridique est nécessaire pour les fournisseurs de services et autres entités concernant les circonstances dans lesquelles ils peuvent répondre à des demandes directes de divulgation de données électroniques émanant des autorités de justice pénale d'autres Parties ;

Entendant donc renforcer encore la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques grâce à des outils supplémentaires relevant d'une entraide plus efficace et d'autres formes de coopération entre autorités compétentes ; la coopération en situation d'urgence ; et la coopération directe entre autorités compétentes et fournisseurs de services et autres entités qui possèdent ou contrôlent les informations pertinentes ;

Convaincus que des conditions et garanties efficaces en matière de protection des droits de l'homme et des libertés fondamentales sont bénéfiques pour une coopération transfrontalière efficace aux fins de la justice pénale, y compris entre les secteurs public et privé ;

Reconnaissant que le recueil de preuves électroniques pour les enquêtes pénales concerne souvent des données à caractère personnel, et reconnaissant l'exigence, dans de nombreuses Parties, de protéger la vie privée et les données à caractère personnel afin de satisfaire à leurs obligations constitutionnelles et internationales ; et

Conscients de la nécessité de garantir que les mesures de justice pénale en vigueur concernant la cybercriminalité et le recueil de preuves sous forme électronique sont soumises à des conditions et des garanties pour la protection appropriée des droits de l'homme et des libertés fondamentales, y compris des droits découlant d'obligations que les États ont contractées conformément à des instruments internationaux applicables en matière de droits de l'homme tels que la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe de 1950 (STE n° 5), le Pacte international relatif aux droits civils et politiques des Nations Unies de 1966, la Charte africaine des droits de l'homme et des peuples de 1981, la Convention américaine relative aux droits de l'homme de 1969 et d'autres traités internationaux relatifs aux droits de l'homme ;

Sont convenus de ce qui suit :

Chapitre I – Dispositions communes

Article 1 – But

Le présent Protocole a pour but de compléter :

- a. la Convention entre les Parties au présent Protocole ; et
- b. le Premier Protocole entre les Parties au présent Protocole qui sont aussi Parties au Premier Protocole.

Article 2 – Champ d'application

1. Sauf dispositions contraires prévues au présent Protocole, les mesures qu'il énonce s'appliquent :

- a. pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant

des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique ; et

b. pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations entérinées dans le présent Protocole.

Article 3 – Définitions

1. Les définitions indiquées aux articles 1 et 18, paragraphe 3, de la Convention s'appliquent au présent Protocole.

2. Aux fins du présent Protocole, les définitions supplémentaires ci-dessous s'appliquent :

a. l'expression « autorité centrale » s'entend de l'autorité ou des autorités désignées en vertu d'un traité ou d'un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, ou, à défaut, de l'autorité ou des autorités désignées par une Partie aux termes de l'article 27, paragraphe 2. a., de la Convention ;

b. l'expression « autorité compétente » signifie une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par le présent Protocole aux fins du recueil ou de la production de preuves concernant des enquêtes ou procédures pénales spécifiques ;

c. le terme « urgence » signifie une situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique ;

d. par « données à caractère personnel » on entend les informations relatives à une personne physique identifiée ou identifiable ;

e. l'expression « Partie transférante » désigne la Partie qui transmet les données en réponse à une demande ou dans le cadre d'une équipe d'enquête commune, ou, aux fins de la section 2 du chapitre II, une Partie sur le territoire de laquelle se trouve un fournisseur de services en mesure de les transmettre ou une entité fournissant des services d'enregistrement de noms de domaine.

Article 4 – Langue

1. Les demandes, les injonctions et les renseignements qui les accompagnent présentés à une Partie doivent être rédigés dans une langue acceptable pour la Partie requise ou la Partie à laquelle ils sont notifiés en vertu de l'article 7, paragraphe 5, ou être accompagnés d'une traduction dans cette langue.
2. Les injonctions visées à l'article 7 et les demandes visées à l'article 6 et toute information qui les accompagne seront :
 - a. rédigées dans une langue de l'autre Partie dans laquelle le fournisseur de services ou l'entité les accepte en vertu d'une procédure nationale comparable ;
 - b. rédigées dans une autre langue acceptable pour le fournisseur de services ou l'entité ; ou
 - c. accompagnées d'une traduction dans l'une des langues visées aux paragraphes 2.a ou 2.b.

Chapitre II - Mesures de coopération renforcée

Section 1 – Principes généraux applicables au chapitre II

Article 5 – Principes généraux applicables au chapitre II

1. Conformément aux dispositions du présent chapitre, les Parties s'assurent la coopération mutuelle la plus large possible.
2. La section 2 du présent chapitre se compose des articles 6 et 7. Elle prévoit des procédures renforçant la coopération directe avec les fournisseurs et les entités sur le territoire d'une autre Partie. La section 2 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées.
3. La section 3 du présent chapitre est constituée des articles 8 et 9. Elle prévoit des procédures visant à renforcer la coopération internationale entre les autorités pour la divulgation de données informatiques stockées. La section 3 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.
4. La section 4 du présent chapitre est constituée de l'article 10. Elle prévoit des procédures relatives à l'entraide d'urgence. La section 4 s'applique qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.

5. La section 5 du présent chapitre est constituée des articles 11 et 12. La section 5 s'applique en l'absence de traité ou d'arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise. Les dispositions de la section 5 ne s'appliquent pas lorsqu'un traité ou un arrangement de ce type existe, sauf dans les cas prévus à l'article 12, paragraphe 7. Toutefois, les Parties concernées peuvent convenir d'appliquer les dispositions de la section 5 en lieu et place de celles prévues par le traité ou l'arrangement si celui-ci ne l'interdit pas.

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

7. Les dispositions du présent chapitre ne restreignent pas la coopération entre les Parties, ou entre les Parties et les fournisseurs de services ou d'autres entités, en vertu d'autres accords, arrangements, pratiques ou du droit interne applicables.

Section 2 – Procédures renforçant la coopération directe avec les fournisseurs et les entités dans les autres Parties

Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habilitier ses autorités compétentes aux fins d'enquêtes ou de procédures pénales spécifiques, à émettre auprès d'une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie une demande d'informations en la possession ou sous le contrôle de l'entité en vue d'identifier ou de contacter la personne ayant enregistré un nom de domaine.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à une entité située sur son territoire de divulguer de telles informations en réponse à une demande introduite en vertu du paragraphe 1, sous réserve des conditions raisonnables prévues par le droit interne.

3. La demande visée au paragraphe 1 doit comporter :

- a. la date d'émission de la requête, l'identité et les coordonnées de l'autorité émettrice compétente;
 - b. le nom de domaine pour lequel les informations sont demandées et une liste détaillée des informations demandées, y compris les éléments de données particuliers;
 - c. une mention déclarant que la demande est émise en vertu du présent Protocole et que l'information est nécessaire du fait de la pertinence qu'elle revêt pour une enquête ou procédure pénale spécifique et que l'information ne sera utilisée que dans le cadre de cette enquête ou procédure pénale spécifique; et
 - d. le délai et le moyen de divulgation de ces informations et toutes autres instructions procédurales spéciales.
4. Si l'entité le juge acceptable, une Partie peut présenter une demande au titre du paragraphe 1 sous forme électronique. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.
 5. Si une entité visée au paragraphe 1 ne coopère pas, la Partie requérante peut lui demander de motiver la non-divulgation des informations demandées. La Partie requérante peut envisager une consultation avec la Partie sur le territoire de laquelle l'entité est située en vue de déterminer les mesures disponibles pour obtenir les informations.
 6. Chaque Partie, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, communique au Secrétaire Général du Conseil de l'Europe l'autorité désignée aux fins de consultation en vertu du paragraphe 5.
 7. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 6. Chaque Partie veille à ce que les informations qu'elle a fournies pour le registre soient exactes à tout moment.

Article 7 – Divulgation de données relatives aux abonnés

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habilitier ses autorités compétentes à adresser directement à un fournisseur de services sur le territoire d'une autre Partie une injonction de produire des données spécifiées et stockées relatives à des abonnés, en la possession ou sous le contrôle dudit fournisseur de services, lorsque ces

informations sont nécessaires à des enquêtes ou des procédures pénales spécifiques menées par la Partie émettrice.

2 a. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour qu'un fournisseur de services sur son territoire communique des données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1.

b. Au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut – en ce qui concerne les injonctions adressées aux fournisseurs de services sur son territoire – faire la déclaration suivante: « l'injonction adressée en application de l'article 7, paragraphe 1, doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante. »

3. L'injonction, adressée en application du paragraphe 1 doit comprendre :

- a. l'autorité émettrice et la date d'émission ;
- b. une déclaration indiquant que l'injonction est émise en vertu du présent Protocole ;
- c. le nom et l'adresse du ou des fournisseurs de services visés ;
- d. la ou les infractions faisant l'objet de l'enquête ou de la procédure pénale ;
- e. l'autorité qui sollicite les données spécifiques relatives aux abonnés, s'il ne s'agit pas de l'autorité émettrice ; et
- f. les données spécifiques relatives aux abonnés qui sont demandées, au moyen d'une description détaillée.

4. L'injonction adressée en application du paragraphe 1 doit être accompagnée des informations complémentaires suivantes :

- a. le fondement juridique interne qui habilite l'autorité à adresser une injonction ;
- b. la mention des dispositions juridiques et des sanctions applicables à l'infraction qui est à l'origine d'une enquête ou de poursuites ;
- c. les coordonnées de l'autorité à laquelle le fournisseur de services doit communiquer les données relatives aux abonnés, à laquelle il peut demander de plus amples informations ou adresser toute autre réponse ;
- d. le délai et le mode de communication des données relatives aux abonnés ;

e. l'indication d'une éventuelle demande de conservation des données précédemment formulée, en précisant la date de conservation et tout numéro de référence applicable;

f. tout type d'instructions spéciales en matière de procédure; et

g. le cas échéant, une déclaration selon laquelle la notification simultanée a été faite conformément au paragraphe 5; et

h. toute autre information qui pourrait aider à obtenir la divulgation des données relatives aux abonnés.

5 a. Une Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, notifier au Secrétaire Général du Conseil de l'Europe qu'elle exige, lorsqu'une injonction est adressée en application du paragraphe 1 à un fournisseur de services sur son territoire, dans chaque cas ou dans certaines circonstances déterminées, la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure.

b. Qu'une Partie exige ou non la communication d'informations prévue au paragraphe 5.a, elle peut, dans certaines circonstances déterminées, demander au fournisseur de services de consulter les autorités de la Partie avant de divulguer les données demandées.

c. Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b peuvent, dans les plus brefs délais, enjoindre au fournisseur de services de ne pas divulguer les données demandées, si:

- i. cette divulgation risque de porter préjudice à des enquêtes ou procédures pénales menées sur le territoire de cette Partie; ou
- ii. les conditions ou les motifs de refus visés aux articles 25, paragraphe 4, et 27, paragraphe 4, de la Convention s'appliquent parce que les données relatives aux abonnés ont fait l'objet d'une demande d'entraide.

d. Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b:

- i. peuvent demander des informations complémentaires à l'autorité visée au paragraphe 4.c aux fins de l'application du paragraphe 5.c et ne les divulgueront pas au fournisseur de services sans le consentement de cette autorité; et

ii. doivent informer rapidement l'autorité visée au paragraphe 4.c si le fournisseur de services a reçu pour instruction de ne pas divulguer les données demandées et doivent motiver cette décision.

e. Une Partie doit désigner une autorité unique pour recevoir la communication prévue au paragraphe 5.a et exécuter les tâches décrites aux paragraphes 5.b, 5.c. et 5.d. La Partie communique au Secrétaire Général du Conseil de l'Europe, au moment où la notification au Secrétaire Général prévue au paragraphe 5.a est faite pour la première fois, les coordonnées de cette autorité.

f. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties conformément au paragraphe 5.e et note si elles exigent la communication d'informations prévue au paragraphe 5.a et dans quelles circonstances. Chaque Partie veille à ce que les informations qu'elle a fournies pour le registre soient exactes à tout moment.

6. Si le fournisseur de services le juge acceptable, une Partie peut soumettre sous forme électronique une injonction au titre du paragraphe 1 et des informations complémentaires au titre du paragraphe 4. Une Partie peut fournir sous forme électronique la notification et les informations complémentaires au titre du paragraphe 5. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.

7. Si un fournisseur de services informe l'autorité visée au paragraphe 4.c qu'il ne divulguera pas les données demandées relatives aux abonnés ou s'il ne divulgue pas les données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1 dans les trente jours suivant sa réception ou dans le délai prévu au paragraphe 4.d, la plus longue période étant retenue, les autorités compétentes de la Partie émettrice peuvent ensuite demander l'exécution de leur injonction uniquement au moyen de l'article 8 ou d'autres formes d'entraide. Les Parties peuvent demander au fournisseur de services de motiver son refus de divulguer les données relatives aux abonnés qui font l'objet de l'injonction.

8. Une Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'une Partie émettrice doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en vertu de l'article 8, à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait.

9. Au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut :

- a. se réserver le droit de ne pas appliquer le présent article ; ou
- b. si la divulgation de certains types de numéros d'accès en vertu du présent article était incompatible avec les principes fondamentaux de son ordre juridique interne, se réserver le droit de ne pas appliquer le présent article à ces numéros.

Section 3 – Procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées

Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux abonnés et au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à délivrer une injonction à présenter dans le cadre d'une demande à une autre Partie afin d'ordonner à un fournisseur de services sur le territoire de la Partie requise de communiquer

- a. des informations relatives à un abonné, et
- b. des données relatives au trafic spécifiées et stockées, en la possession ou sous le contrôle dudit fournisseur de services, lorsque ces informations et données sont nécessaires pour des enquêtes ou procédures pénales spécifiques menées par la Partie.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour donner effet à une injonction visée au paragraphe 1 soumise par une Partie requérante.

3. Dans sa demande, la Partie requérante soumet l'injonction visée au paragraphe 1, les informations qui l'accompagnent et toute instruction procédurale spéciale à la Partie requise.

- a. L'injonction doit comprendre :
 - i. l'autorité émettrice et la date d'émission de la requête ;
 - ii. une déclaration selon laquelle l'injonction est soumise en vertu du présent Protocole ;
 - iii. le nom et l'adresse du ou des fournisseurs de services à laquelle elle doit être notifiée ;

- iv la ou les infractions visées par l'enquête ou la procédure pénale;
 - v l'autorité à l'origine de la demande d'informations ou de données, si elle est différente de l'autorité ayant délivré l'injonction; et
 - vi. de manière détaillée les informations ou les données spécifiques demandées.
- b. Les informations fournies à l'appui de l'injonction pour aider la Partie requise à lui donner effet et qui ne doivent pas être divulguées au fournisseur de services sans le consentement de la Partie requérante doivent comprendre:
- i. les fondements juridiques en droit interne qui donnent à l'autorité le pouvoir d'émettre l'injonction;
 - ii. les dispositions légales et les sanctions applicables pour la ou les infractions objet de l'enquête ou des poursuites;
 - iii. la raison pour laquelle la Partie requérante pense que le fournisseur de services est en possession des données ou les contrôle;
 - iv une synthèse des faits liés à l'enquête ou aux poursuites;
 - v la pertinence des informations ou données pour l'enquête ou la procédure;
 - vi. les éléments permettant de contacter une ou des autorités pour de plus amples informations;
 - vii. si la conservation des informations ou des données a déjà été demandée, auquel cas le document précisera la date de la demande et la cote de référence; et
 - viii. si les informations ou les données ont déjà été demandées par d'autres moyens et si oui, de quelle manière.
- c. La Partie requérante peut demander que la Partie requise suive des instructions procédurales spéciales.
4. Une Partie peut déclarer au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, et à tout autre moment, que des informations complémentaires sont nécessaires pour donner effet à des injonctions soumises en vertu du paragraphe 1.
5. La Partie requise accepte les demandes sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

6 a. À compter de la date de réception de toutes les informations visées aux paragraphes 3 et 4, la Partie requise s'emploie raisonnablement à notifier l'injonction au fournisseur de services dans les quarante-cinq jours au plus en lui ordonnant de produire les informations en retour dans les :

- i. vingt jours pour des informations relatives à l'abonné ; et
- ii. quarante-cinq jours pour les données relatives au trafic.

b. La Partie requise procède sans tarder à la transmission à la Partie requérante des informations ou données produites.

7. Si la Partie requise n'est pas en mesure d'appliquer sous la forme requise les instructions visées au paragraphe 3.c, elle en informe sans délai la Partie requérante et, au besoin, spécifie les conditions qui lui permettraient d'appliquer les instructions, à la suite de quoi la Partie requérante détermine si la demande doit malgré tout être exécutée.

8. La Partie requise peut invoquer les motifs visés à l'article 25, paragraphe 4, ou à l'article 27, paragraphe 4, de la Convention pour refuser l'exécution d'une demande ou peut imposer les conditions qu'elle estime nécessaires pour permettre l'exécution de la demande. La Partie requise peut invoquer les raisons visées à l'article 27, paragraphe 5, de la Convention pour ajourner l'exécution d'une demande. La Partie requise notifie dès que possible le refus, les conditions ou l'ajournement à la Partie requérante. La Partie requise notifie également à la Partie requérante les autres circonstances pouvant retarder de manière significative l'exécution de la demande. L'article 28, paragraphe 2.b de la Convention s'applique au présent article.

9 a. Si la Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 8, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou le matériel devraient néanmoins être fournis.

b. Si la Partie requérante accepte la condition, elle est liée par celle-ci. La Partie requise qui fournit des informations ou du matériel soumis à une telle condition peut exiger de la Partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces informations ou de ce matériel.

10. Au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, chaque Partie communique au Secrétaire Général du Conseil de l'Europe et tient à jour les coordonnées des autorités désignées :

- a. pour soumettre une injonction visée par le présent article ; et
- b. pour recevoir une injonction visée par le présent article.

11. Une Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige que les demandes des autres Parties visées par le présent article soient transmises par l'autorité centrale de la Partie requérante, ou par toute autre autorité désignée d'un commun accord entre les Parties concernées.

12. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 10. Chaque Partie veille à ce que les informations qu'elle a fournies pour le registre soient exactes à tout moment.

13. Au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut se réserver le droit de ne pas appliquer le présent article aux données relatives au trafic.

Article 9 – Divulgence accélérée de données informatiques stockées en situation d'urgence

1.a. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires, en cas d'urgence, pour que son point de contact du Réseau 24/7 visé à l'article 35 de la Convention (« point de contact ») puisse transmettre une demande à un point de contact dans une autre Partie et recevoir une demande de ce dernier pour une assistance immédiate en vue de l'obtention par un fournisseur de services situé sur le territoire de la Partie concernée de la divulgation accélérée de données informatiques stockées spécifiées qui sont en la possession ou sous le contrôle dudit fournisseur de services, sans requête d'entraide judiciaire.

b. Une Partie peut, au moment de la signature du présent Protocole ou au moment du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle n'exécutera pas de demandes introduites en vertu du paragraphe 1.a pour la divulgation d'informations relatives à l'abonné seulement.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter, conformément au paragraphe 1 :

- a. ses autorités à demander des données à un fournisseur de services situé sur son territoire à la suite d'une demande émise en vertu du paragraphe 1 ;
 - b. un fournisseur de services sur son territoire à divulguer les données demandées à ses autorités en réponse à une demande émise en vertu du paragraphe 2.a ; et
 - c. ses autorités à fournir les données demandées à la Partie requérante.
3. La demande introduite en vertu du paragraphe 1 :
- a. spécifie l'autorité compétente qui cherche des données et la date à laquelle la demande a été faite ;
 - b. contient une déclaration selon laquelle la demande est émise en vertu du présent Protocole ;
 - c. précise le nom et l'adresse du/des fournisseur(s) de services en possession des données recherchées ou qui en ont le contrôle ;
 - d. précise la ou les infractions faisant l'objet de l'enquête ou des procédures pénales et indique la référence à ses dispositions légales et les sanctions applicables ;
 - e. mentionne suffisamment de faits démontrant que la situation est urgente et comment les données demandées sont liées à la situation ;
 - f. s'accompagne d'une description détaillée des données demandées ;
 - g. précise les éventuelles instructions procédurales ; et
 - h. mentionne toute autre information pouvant aider à obtenir la divulgation des données demandées.
4. La Partie requise accepte des demandes sous forme électronique. Une Partie peut également accepter des demandes transmises oralement et peut exiger une confirmation sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.
5. Une Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige des Parties requérantes que celles-ci, après l'exécution de la demande, lui soumettent la demande et toutes informations supplémentaires transmises à l'appui de cette dernière, selon le format et le canal, qui peut couvrir une demande d'entraide judiciaire, spécifiés par la Partie requise.

6. La Partie requise informe la Partie requérante selon une procédure accélérée de sa détermination concernant la demande visée au paragraphe 1 et, au besoin, spécifie les éventuelles conditions auxquelles elle fournirait les données et toutes autres formes de coopération qui peuvent être utilisées.

7. a Si une Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 6, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou les documents devraient néanmoins être fournis. Si la Partie requérante accepte la condition, elle est liée par celle-ci.

b. La Partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la Partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ce matériel.

Section 4 – Procédures relatives à la demande d'entraide urgente

Article 10 – Demande d'entraide urgente

1. Chaque Partie peut demander une entraide judiciaire par les moyens les plus rapides lorsqu'elle estime qu'il y a urgence. Une demande d'entraide en vertu du présent article doit présenter, outre les autres contenus requis, une description des faits étayant l'existence d'une situation urgente et une explication de la manière dont l'entraide demandée est liée à cette situation.

2. La Partie requise accepte une telle demande d'entraide sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

3. La Partie requise peut, par les moyens les plus rapides, demander un complément d'information afin d'évaluer la demande d'entraide. La Partie requérante fournit ce complément d'information par les moyens les plus rapides.

4. Après avoir conclu à l'existence d'une situation urgente et s'être assurée que les autres conditions de l'entraide sont satisfaites, la Partie requise répond à la demande d'entraide par les moyens les plus rapides.

5. Chaque Partie veille à ce qu'une personne de son autorité centrale ou d'autres autorités responsables des demandes d'entraide soit disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour répondre à une demande présentée en vertu du présent article.

6. L'autorité centrale ou les autres autorités responsables des demandes d'entraide des Parties requérante et requise peuvent décider de prévoir que les résultats de l'exécution d'une demande d'entraide effectuée en vertu du présent article, ou une copie préliminaire de ces résultats, peuvent être transmis à la Partie requérante par un canal autre que celui utilisé pour la transmission la demande.

7. Lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, l'article 27, paragraphes 2.b et 3 à 8, et l'article 28, paragraphes 2 à 4, de la Convention s'appliquent au présent article.

8. Lorsqu'un tel traité ou arrangement existe, le présent article est complété par les dispositions de ce traité ou arrangement, à moins que les Parties concernées ne décident d'un commun accord d'appliquer à la place l'une ou la totalité des dispositions de la Convention visées au paragraphe 7 du présent article.

9. Chaque Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que des demandes d'entraide peuvent aussi être adressées directement par ses autorités judiciaires, ou par le biais de l'Organisation internationale de police criminelle (INTERPOL) ou du point de contact 24/7 établi au titre de l'article 35 de la Convention. Dans de tels cas, une copie est envoyée en même temps à l'autorité centrale de la Partie requise par le truchement de l'autorité centrale de la Partie requérante. Lorsqu'une demande est adressée directement à une autorité judiciaire de la Partie requise et que celle-ci n'est pas compétente pour traiter la demande, elle transmet la demande à l'autorité nationale compétente et en informe directement la Partie requérante.

Section 5 – Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

Article 11 – Vidéoconférence

1. Une Partie requérante peut demander, et la Partie requise peut autoriser, le recueil de la déposition d'un témoin ou d'un expert par vidéoconférence. La Partie requérante et la Partie requise se concertent pour faciliter le règlement de toutes les questions pouvant se poser concernant l'exécution de la demande, y compris le cas échéant le choix de la Partie qui préside la

séance; les autorités et personnes qui doivent être présentes; si l'une des Parties ou les deux doivent demander au témoin ou à l'expert de prêter un serment particulier, lui dispenser des avertissements ou des instructions; la manière d'interroger le témoin ou l'expert; la manière permettant de garantir dûment les droits du témoin ou de l'expert; le traitement des revendications de privilèges ou d'immunité; le traitement des objections aux questions ou réponses; et la question de savoir si l'une des Parties ou les deux assurent des services de traduction, d'interprétation et de transcription.

2. a. Les autorités centrales de la Partie requise et de la Partie requérante communiquent directement entre elles aux fins du présent article. Une Partie requise peut accepter une demande sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

b. La Partie requise informe la Partie requérante des raisons pour lesquelles la demande n'a pas été exécutée ou a été retardée. L'article 27, paragraphe 8, de la Convention s'applique au présent article. Sans préjudice de toute autre condition qu'une Partie requise peut imposer conformément au présent article, les paragraphes 2 à 4 de l'article 28 de la Convention s'appliquent au présent article.

3. Une Partie requise fournissant son assistance au titre du présent article veille aux mesures nécessaires pour obtenir la présence de la personne dont le témoignage ou la déposition est requis. Le cas échéant, la Partie requise peut, dans la mesure où son droit le lui permet, prendre les mesures nécessaires pour obliger un témoin ou un expert à comparaître dans la Partie requise à l'endroit, à la date et à l'heure fixées.

4. Les procédures concernant la conduite de la vidéoconférence spécifiées par la Partie requérante sont appliquées, à moins qu'elles ne soient incompatibles avec le droit interne de la Partie requise. En cas d'incompatibilité, ou si la procédure n'a pas été spécifiée par la Partie requérante, la Partie requise applique la procédure prévue dans son droit interne sauf s'il en a été convenu autrement par les Parties requérante et requise.

5. Sans préjudice d'une éventuelle compétence en vertu du droit interne de la Partie requérante, lorsque, durant la vidéoconférence, le témoin ou l'expert :

a. fait intentionnellement une fausse déclaration alors que la Partie requise lui a, conformément à son droit interne, intimé de dire la vérité dans sa déposition;

b. refuse de témoigner alors que la Partie requise l'a, conformément à son droit interne, astreint à le faire ; ou

c. commet tout autre acte interdit par le droit interne de la Partie requise au cours de l'audition ;

il encourt dans la Partie requise la même sanction que si l'acte avait été commis dans le cadre des procédures prévues par le droit interne de cette dernière.

6. a. À moins que la Partie requérante et la Partie requise en aient décidé autrement, la Partie requise supporte tous les coûts liés à l'exécution d'une demande d'entraide en vertu du présent article, sauf :

- i. les honoraires d'un témoin expert ;
- ii. les coûts de traduction, d'interprétation et de transcription ; et
- iii. les dépenses exceptionnelles.

b. Si l'exécution d'une demande est susceptible d'entraîner des dépenses de nature exceptionnelle, la Partie requérante et la Partie requise se concertent pour déterminer les conditions auxquelles la demande sera exécutée.

7. Lorsque la Partie requérante et la Partie requise en conviennent :

a. les dispositions du présent article peuvent être appliquées dans le but de réaliser des audioconférences ;

b. la technologie de la vidéoconférence peut être utilisée à des fins, ou pour des auditions, différentes de celles visées au paragraphe 1, y compris en vue de l'identification de personnes ou d'objets.

8. Lorsqu'une Partie requise choisit d'autoriser l'audition d'un suspect ou d'un inculpé, elle peut poser des conditions et garanties particulières pour ce qui est du recueil du témoignage ou de la déposition de la personne, ou prévoir des notifications ou applications de mesures procédurales concernant cette personne.

Article 12 – Équipes communes d'enquête et enquêtes communes

1. Lorsqu'une coordination renforcée est considérée comme particulièrement utile, d'un commun accord, les autorités compétentes de deux ou plusieurs Parties peuvent établir et faire fonctionner une équipe commune d'enquête sur leurs territoires pour faciliter les enquêtes ou les poursuites. Les autorités compétentes sont déterminées par les Parties respectives concernées.

2. Les procédures et modalités régissant le fonctionnement d'équipes communes d'enquête, telles que leurs objectifs spécifiques ; leur composition ; leurs fonctions ; leur durée et toute éventuelle prolongation ; leur emplacement ; leur organisation ; le recueil, la transmission et l'utilisation des informations ou preuves ; les conditions de confidentialité et les conditions de l'implication des autorités participantes d'une Partie dans des mesures d'enquête se déroulant sur le territoire d'une autre Partie, font l'objet d'un accord entre les autorités compétentes concernées.

3. Une Partie peut déclarer, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, que son autorité centrale doit être signataire de l'accord portant création de l'équipe ou y souscrire d'une autre manière.

4. Ces autorités compétentes et participantes communiquent directement entre elles, mais les Parties peuvent convenir d'autres canaux de communication appropriés lorsque des circonstances exceptionnelles requièrent une coordination plus centrale.

5. Lorsque des mesures d'enquête doivent être prises sur le territoire de l'une des Parties concernées, les autorités participantes de cette Partie peuvent demander à leurs propres autorités de prendre ces mesures sans que les autres Parties aient à soumettre une demande d'entraide. Ces mesures doivent être mises en œuvre par les autorités de cette Partie sur son territoire aux conditions s'appliquant en droit interne à une enquête nationale.

6. L'utilisation d'informations ou de preuves fournies par les autorités participantes d'une Partie aux autorités participantes d'autres Parties concernées peut être refusée ou limitée dans les conditions prévues à l'accord décrit aux paragraphes 1 et 2. Si un tel accord ne prévoit pas de conditions pour le refus ou la limitation de cette utilisation, les Parties peuvent utiliser les informations ou preuves fournies :

- a. aux fins pour lesquelles l'accord a été conclu ;
- b. pour détecter, enquêter sur et poursuivre des infractions pénales autres que celles pour lesquelles l'accord a été conclu, sous réserve du consentement préalable des autorités qui ont fourni ces informations ou preuves. Le consentement ne sera toutefois pas requis lorsque les principes juridiques fondamentaux de la Partie utilisant les informations ou preuves exigent qu'elle divulgue ces dernières pour protéger les droits d'une personne poursuivie dans le cadre d'une procédure pénale. Dans ce cas, les autorités concernées

doivent le notifier sans retard indu aux autorités qui ont fourni les informations ou preuves ; ou

c. pour leur permettre de prévenir une urgence. Dans ce cas, les autorités participantes qui ont reçu les informations ou preuves doivent le notifier dans les plus brefs délais aux autorités participantes qui les ont fournies, sauf autre accord.

7. En l'absence d'accord tel que visé aux paragraphes 1 et 2, des enquêtes conjointes peuvent être mises en œuvre selon des modalités convenues au cas par cas. Le présent paragraphe s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les Parties concernées.

Chapitre III – Conditions et garanties

Article 13 – Conditions et garanties

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.

Article 14 – Protection des données à caractère personnel

1. Champ d'application

a. Sauf disposition contraire des paragraphes 1.b et c, chaque Partie traite les données à caractère personnel qu'elle reçoit au titre du présent Protocole conformément aux paragraphes 2 à 15 du présent article.

b. Si, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie transférante et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application de cet accord, aux données à

caractère personnel reçues en vertu du présent Protocole en lieu et place des paragraphes 2 à 15, sauf accord contraire entre les Parties concernées.

c. Si la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord décrit au paragraphe 1.a, elles peuvent déterminer d'un commun accord que le transfert de données à caractère personnel en vertu du présent Protocole peut avoir lieu sur la base d'autres accords ou arrangements entre les Parties concernées en lieu et place des paragraphes 2 à 15.

d. Chaque Partie considère que le traitement des données à caractère personnel conformément aux paragraphes 1.a et 1.b répond aux exigences de son cadre juridique de protection des données à caractère personnel pour les transferts internationaux de données à caractère personnel, et aucune autre autorisation de transfert n'est requise en vertu de ce cadre juridique. Une Partie ne peut refuser ou empêcher les transferts de données vers une autre Partie en vertu du présent Protocole que pour des raisons de protection des données: dans les conditions énoncées au paragraphe 15, lorsque le paragraphe 1.a s'applique; ou aux termes d'un accord ou d'un arrangement visé aux paragraphes 1.b ou c, lorsque l'un de ces paragraphes s'applique.

e. Aucune disposition du présent article n'empêche une Partie d'appliquer des garanties plus strictes au traitement par ses propres autorités des données à caractère personnel reçues en vertu du présent Protocole.

2. But et utilisation

a. La Partie destinataire de données à caractère personnel traite lesdites données aux fins prévues à l'article 2. Elle ne procède pas à d'autres traitements des données à caractère personnel dans un but incompatible avec cet article, et elle ne traite pas non plus les données lorsque son cadre juridique interne ne l'autorise pas. Le présent article ne porte pas atteinte à la capacité de la Partie transférante d'imposer des conditions complémentaires en vertu du présent Protocole dans une situation spécifique; toutefois, ces conditions n'incluent pas des conditions génériques de protection des données.

b. La Partie destinataire veille, dans son cadre juridique interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement.

3. Qualité et intégrité

Chaque Partie prend des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte

et complète et soient aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi, compte tenu des buts dans lesquels elles sont traitées.

4. Données sensibles

Le traitement par une Partie de données à caractère personnel révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale, ainsi que le traitement de données génétiques, de données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent ; ou de données à caractère personnel concernant la santé ou la sexualité ; ne peut avoir lieu que moyennant des garanties appropriées pour se prémunir contre le risque d'effets préjudiciables injustifiés résultant de l'utilisation de ces données, en particulier contre la discrimination illicite.

5. Durées de conservation

Chaque Partie conserve les données à caractère personnel uniquement pour la durée nécessaire et appropriée, aux fins du traitement des données prévu au paragraphe 2. Pour s'acquitter de cette obligation, la Partie prévoit dans son cadre juridique interne des durées de conservation spécifiques ou une révision périodique de la nécessité de continuer à conserver les données.

6. Décisions automatisées

Les décisions ayant un effet défavorable significatif sur les intérêts pertinents de l'individu concerné par les données à caractère personnel ne peuvent pas être fondées uniquement sur un traitement automatisé des données à caractère personnel, sauf autorisation dans le droit interne et avec des garanties appropriées qui prévoient la possibilité d'obtenir une intervention humaine.

7. Sécurité des données et incidents de sécurité

a. Chaque Partie s'assure de disposer de mesures technologiques, physiques et organisationnelles appropriées pour la protection des données à caractère personnel, en particulier contre la perte ou l'accès, la divulgation, l'altération ou la destruction accidentels ou non autorisés (« incident lié à la sécurité »).

b. Dès qu'il est pris connaissance d'un incident de sécurité entraînant un risque significatif de préjudice matériel ou non matériel à des personnes ou à l'autre Partie, la Partie qui a reçu les données en évalue sans tarder la probabilité de survenance et l'importance, et prend rapidement les mesures appropriées pour atténuer ce préjudice. Ces mesures prennent la forme d'une notification à l'autorité transférante ou, aux fins du chapitre II, section 2, à l'autorité ou aux

autorités désignées conformément au paragraphe 7.c. Cependant, la notification peut prévoir des restrictions appropriées concernant la transmission ultérieure de la notification ; elle peut être différée ou omise lorsqu'elle risque de porter atteinte à la sécurité nationale, ou être retardée lorsque cette notification peut mettre en danger des opérations visant à protéger la sécurité publique. Ces mesures doivent également inclure une notification à la personne concernée, à moins que la Partie n'ait pris des mesures appropriées afin qu'il n'y ait plus de risque significatif. La notification à la personne concernée peut être différée ou omise dans les conditions énoncées au paragraphe 12.a.i. La Partie qui reçoit la notification peut demander une consultation et un complément d'information concernant l'incident et la réponse qui a été mise en œuvre.

c. Chaque Partie, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, indique au Secrétaire Général du Conseil de l'Europe quelles sont l'autorité ou les autorités qui reçoivent la notification visée au paragraphe 7.b, aux fins de la section 2 du chapitre II ; celles-ci peuvent être modifiées ultérieurement.

8. Tenue des registres

Chaque Partie tient des registres ou se dote d'autres moyens appropriés pour montrer comment il est accédé aux données à caractère personnel d'un individu et comment celles-ci sont utilisées et divulguées dans un cas spécifique.

9. Partage ultérieur au sein d'une Partie

a. Lorsqu'une autorité d'une Partie fournit des données à caractère personnel reçues initialement en vertu du présent Protocole à une autre autorité de cette Partie, cette dernière les traite conformément au présent article, sous réserve du paragraphe 9.b.

b. Nonobstant le paragraphe 9.a, une Partie qui a fait une réserve en vertu de l'article 17 peut fournir des données à caractère personnel qu'elle a reçues à ses États constitutifs ou à des entités territoriales similaires, à condition que la Partie ait mis en place des mesures pour que les autorités qui reçoivent les données continuent à les protéger efficacement en assurant un niveau de protection des données comparable à celui offert par le présent article.

c. En cas d'indications d'une application incorrecte du présent paragraphe, la Partie transférante peut demander une consultation et des informations pertinentes sur ces indications.

10. Transfert ultérieur vers un autre État ou vers une organisation internationale

a. La Partie recevant les données à caractère personnel ne peut les transférer à un autre État ou à une organisation internationale qu'avec l'autorisation préalable de l'autorité qui les lui a communiquées ou, aux fins de la section 2 du chapitre II, de l'autorité ou des autorités désignées en vertu du paragraphe 10.b.

b. Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, l'autorité ou les autorités habilitées à autoriser un transfert aux fins de la section 2 du chapitre II; ces informations peuvent être modifiées ultérieurement.

11. Transparence et notification

a. Chaque Partie assure les notifications par publication de notifications générales ou par notification spécifique à l'individu dont les données à caractère personnel ont été recueillies, concernant:

- i. la base juridique et le(s) but(s) du traitement;
- ii. toute durée de conservation ou tout délai de révision tels que visés au paragraphe 5, le cas échéant;
- iii. les destinataires ou les catégories de destinataires auxquels ces informations sont divulguées; et
- iv l'accès, les rectifications ainsi que les recours possibles.

b. Une Partie peut soumettre toute exigence de notification personnelle à des restrictions raisonnables en vertu de son cadre juridique interne conformément aux conditions énoncées au paragraphe 12.a.i.

c. Lorsque le cadre juridique interne de la Partie transférante exige que l'individu dont les données ont été fournies à une autre Partie soit informé personnellement, la Partie transférante prend des mesures pour que l'autre Partie soit informée au moment du transfert de cette exigence et des coordonnées appropriées. La notification personnelle n'est pas effectuée si l'autre Partie a demandé que la fourniture des données demeure confidentielle, dans la mesure où les conditions de restriction définies au paragraphe 12.a.i s'appliquent. Dès que ces restrictions ne s'appliquent plus et que la notification personnelle peut être effectuée, l'autre Partie prend des mesures pour que la Partie transférante soit informée. Si elle n'a pas encore été informée, la Partie transférante peut faire des demandes à la Partie destinataire qui informera la Partie transférante si la restriction doit être maintenue.

12. Accès et rectification

a. Chaque Partie veille à ce que toute personne dont les données à caractère personnel ont été reçues en application du présent Protocole ait le droit de demander et d'obtenir, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif:

- i. l'accès à une copie écrite ou électronique de la documentation conservée sur cette personne, contenant ses données à caractère personnel et les informations disponibles indiquant la base juridique et les finalités du traitement, les périodes de conservation et les destinataires ou catégories de destinataires des données (« accès »), ainsi que les informations concernant les possibilités de recours disponibles à condition que l'accès dans un cas particulier puisse être soumis à l'application de restrictions proportionnées autorisées par son cadre juridique interne, nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée;
- ii. la rectification lorsque les données à caractère personnel de la personne sont inexactes ou ont été traitées de manière inappropriée; la rectification doit inclure, selon ce qui est approprié et raisonnable compte tenu des motifs de la demande de rectification et du contexte particulier du traitement, la correction, le complément, l'effacement ou l'anonymisation, la restriction du traitement ou le blocage.

b. Si l'accès ou la rectification est refusé ou restreint, la Partie informe la personne concernée sous une forme écrite qui peut être envoyée par voie électronique, sans retard excessif, en informant l'individu du refus ou de la restriction. Elle indique les motifs de ce refus ou de cette restriction et fournit des informations sur les voies de recours disponibles. Les frais d'accès doivent être limités à ce qui est raisonnable et non excessif.

13. Recours judiciaire et non-judiciaire

Chaque Partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article.

14. Supervision

Chaque Partie dispose d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et efficaces à l'égard des mesures établies dans le présent article. Les fonctions et compétences exercées ensemble ou séparément par

ces autorités comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives.

15. Consultation et suspension

Une Partie peut suspendre le transfert de données à caractère personnel à une autre Partie si elle dispose de preuves substantielles que celle-ci viole de manière systématique ou flagrante les dispositions du présent article ou qu'une violation flagrante est imminente. Cette suspension n'intervient qu'à l'expiration d'un préavis raisonnable, et pas avant d'avoir engagé une période raisonnable de consultation sans parvenir à une résolution. Toutefois, une Partie peut suspendre provisoirement les transferts en cas de violation systématique ou flagrante présentant un risque important et imminent pour la vie ou la sécurité d'une personne physique, ou un préjudice financier ou de réputation pour cette personne, auquel cas cette Partie en informe l'autre Partie et entame des consultations avec celle-ci immédiatement après. Si les consultations ne permettent pas de trouver une solution, l'autre Partie peut elle aussi suspendre les transferts si elle dispose de preuves substantielles que la suspension mise en œuvre par la première Partie était contraire aux termes du présent paragraphe. La Partie qui a procédé à la suspension la lève dès qu'il a été remédié à la violation justifiant la suspension ; toute suspension réciproque est levée à ce moment. Toutes les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au présent Protocole.

Chapitre IV –Clauses finales

Article 15 – Effets de ce Protocole

1.a. L'article 39, paragraphe 2, de la Convention s'applique au présent Protocole.

b. En ce qui concerne les Parties qui sont membres de l'Union européenne, ces Parties peuvent, dans leurs relations mutuelles, appliquer le droit de l'Union européenne régissant les questions traitées dans le présent protocole.

c. Le paragraphe 1.b n'affecte pas la pleine application du présent Protocole entre les Parties qui sont membres de l'Union européenne et les autres Parties.

2. L'article 39, paragraphe 3, de la Convention s'applique au présent Protocole.

Article 16 – Signature et entrée en vigueur

1. Le présent Protocole est ouvert à la signature des Parties à la Convention, qui peuvent exprimer leur consentement à être liées par :
 - a. la signature sans réserve de ratification, d'acceptation ou d'approbation ;
ou
 - b. la signature sous réserve de ratification, d'acceptation ou d'approbation, suivie de ratification, d'acceptation ou d'approbation.
2. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.
3. Le présent Protocole entre en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Parties à la Convention auront exprimé leur consentement à être liées par le présent Protocole conformément aux dispositions des paragraphes 1 et 2 du présent article.
4. Pour toute Partie à la Convention qui exprime ultérieurement son consentement à être lié par le présent Protocole, celui-ci entre en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle la Partie a exprimé son consentement à être liée par le présent Protocole, conformément aux dispositions des paragraphes 1 et 2 du présent article.

Article 17 – Clause fédérale

1. Un État fédéral peut se réserver le droit d'assumer les obligations découlant du présent Protocole conformément à ses principes fondamentaux régissant les relations entre son gouvernement central et les États constitutifs ou autres entités territoriales similaires, à condition que :
 - a. le présent Protocole s'applique au gouvernement central de l'État fédéral ;
 - b. une telle réserve n'affecte pas les obligations de fournir la coopération demandée par les autres Parties conformément aux dispositions du chapitre II ; et
 - c. les dispositions de l'article 13 s'appliquent aux États constitutifs de l'État fédéral ou aux autres entités territoriales similaires.
2. Une autre Partie peut empêcher les autorités, les fournisseurs ou les entités sur son territoire de coopérer en réponse à une demande ou une

injonction présentée directement par un État constitutif ou une autre entité territoriale similaire d'un État fédéral qui a formulé une réserve en vertu du paragraphe 1, à moins que l'État fédéral ne notifie au Secrétaire Général du Conseil de l'Europe qu'un État constitutif ou une autre entité territoriale similaire applique les obligations du présent Protocole applicables à cet État fédéral. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre de ces notifications.

3. Une autre Partie n'empêche pas les autorités, les fournisseurs ou les entités sur son territoire de coopérer avec un État constitutif ou une autre entité territoriale similaire en raison d'une réserve formulée en vertu du paragraphe 1, si un ordre ou une demande a été soumis par l'intermédiaire du gouvernement central ou si un accord relatif à une équipe commune d'enquête en vertu de l'article 12 est conclu avec la participation du gouvernement central. Dans ces situations, le gouvernement central assure l'exécution des obligations applicables du présent Protocole, étant entendu que, en ce qui concerne la protection des données à caractère personnel fournies aux États constitutifs ou aux entités territoriales similaires, seuls les termes de l'article 14, paragraphe 9, ou, le cas échéant, les termes d'un accord ou d'un arrangement décrit à l'article 14, paragraphes 1.b ou 1.c, s'appliquent.

4. En ce qui concerne les dispositions du présent Protocole dont l'application relève de la compétence des États constitutifs ou d'autres entités territoriales similaires, qui ne sont pas tenus par le système constitutionnel de la fédération de prendre des mesures législatives, le gouvernement central informe les autorités compétentes de ces États desdites dispositions avec son avis favorable, en les encourageant à prendre les mesures appropriées pour leur donner effet.

Article 18 – Application territoriale

1. Le présent Protocole s'applique au territoire ou aux territoires spécifiés dans une déclaration faite par une Partie en vertu de l'article 38, paragraphes 1 ou 2, de la Convention pour autant que cette déclaration n'ait pas été retirée en vertu de l'article 38, paragraphe 3.

2. Une Partie peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que le présent Protocole ne s'applique pas à un ou plusieurs territoires spécifiés dans la déclaration de la Partie en vertu de l'article 38, paragraphes 1 et/ou 2, de la Convention.

3. Une déclaration en vertu du paragraphe 2 du présent article peut, concernant tout territoire qui y est spécifié, être retirée par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait devient effectif le premier jour du mois suivant l'expiration d'une période de trois mois après la date de la réception de cette notification par le Secrétaire Général.

Article 19 – Réserves et déclarations

1. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, déclarer qu'elle se prévaut de la ou des réserves prévues à l'article 7, paragraphes 9.a et 9.b, à l'article 8, paragraphe 13, et à l'article 17 du présent Protocole. Aucune autre réserve ne peut être formulée.

2. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature du présent Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, faire la ou les déclarations prévues à l'article 7, paragraphes 2.b et 8, à l'article 8, paragraphe 11, à l'article 9, paragraphes 1.b et 5, à l'article 10, paragraphe 9, à l'article 12, paragraphe 3, et à l'article 18, paragraphe 2, du présent Protocole.

3. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention fait toute(s) déclaration(s), notifications ou communications visées à l'article 7, paragraphes 5.a et 5.e, à l'article 8, paragraphes 4, 10.a et 10.b, à l'article 14, paragraphes 7.c et 10.b, et à l'article 17, paragraphe 2, du présent Protocole selon les modalités qui y sont spécifiées.

Article 20 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'article 19, paragraphe 1, retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 19, paragraphe 1, des informations sur les perspectives de leur retrait.

Article 21 – Amendements

1. Toute Partie au présent Protocole peut proposer des amendements, qui sont communiqués par le Secrétaire Général du Conseil de l'Europe, aux États membres du Conseil de l'Europe et aux États Parties à la Convention et Signataires de celle-ci ainsi qu'à tout État invité à adhérer à la Convention.
2. Tout amendement proposé par une Partie est communiqué au Comité européen sur les problèmes criminels (CDPC) qui soumet au Comité des Ministres son avis sur cet amendement proposé.
3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Parties à la Convention, peut adopter l'amendement.
4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 est transmis aux Parties au présent Protocole pour acceptation.
5. Tout amendement adopté conformément au paragraphe 3 entre en vigueur le trentième jour après que toutes les Parties au présent Protocole ont informé le Secrétaire Général qu'elles acceptent l'amendement.

Article 22 – Règlement des différends

L'article 45 de la Convention s'applique au présent Protocole.

Article 23 – Consultations des Parties et évaluation de la mise en œuvre

1. L'article 46 de la Convention s'applique au présent Protocole.
2. Les Parties évaluent périodiquement l'utilisation et la mise en œuvre effectives des dispositions du présent Protocole. L'article 2 du Règlement intérieur du Comité de la Convention sur la cybercriminalité tel que révisé le 16 octobre 2020 s'applique mutatis mutandis. Les Parties réexaminent initialement et peuvent modifier par consensus les procédures de cet article telles qu'elles s'appliquent au présent Protocole cinq ans après l'entrée en vigueur du présent Protocole.
3. L'examen de l'article 14 débute lorsque dix Parties à la Convention ont exprimé leur consentement à être liées par le présent Protocole.

Article 24 – Dénonciation

1. Toute Partie peut, à tout moment, dénoncer le présent Protocole par notification au Secrétaire Général du Conseil de l'Europe.
2. Ladite dénonciation prendra effet le premier jour du mois suivant l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.
3. La dénonciation de la Convention par une Partie au présent Protocole constitue une dénonciation du présent Protocole.
4. Les informations ou éléments de preuve transférés avant la date de prise d'effet de la dénonciation continuent d'être traités conformément au présent Protocole.

Article 25 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux États membres du Conseil de l'Europe, aux Parties à la Convention et Signataires de la Convention, et à tout État invité à adhérer à la Convention :

- a. toute signature ;
- b. le dépôt de tout instrument de ratification, d'acceptation ou d'approbation ;
- c. la date d'entrée en vigueur du présent Protocole conformément à l'article 16, paragraphes 3 et 4 ;
- d. toutes déclarations ou réserves formulées conformément à l'article 19 ou retrait de réserves formulé conformément à l'article 20 ;
- e. tout autre acte, notification ou communication concernant le présent Protocole.

En foi de quoi, les soussignés, dûment autorisés, ont apposé leur signature au bas du présent Protocole.

Fait à Strasbourg, le 12 mai 2022, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui est déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe communiquera une copie certifiée conforme à chacun des États membres du Conseil de l'Europe, aux Parties et Signataires de la Convention, ainsi qu'à tout État invité à adhérer à la Convention.

Rapport explicatif du Deuxième Protocole additionnel

1. Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif à une coopération et la divulgation de preuves électroniques renforcée (le « Protocole ») a été adopté par le Comité des Ministres du Conseil de l'Europe lors de sa 1417^e bis réunion (17 novembre 2021) des Délégués des Ministres et le Protocole sera ouvert à la signature à Strasbourg, le 12 mai 2022. Le Comité des Ministres a également pris note du rapport explicatif.
2. Le texte du présent rapport explicatif est destiné à guider et à aider les Parties dans l'application du présent Protocole et reflète la compréhension des rédacteurs quant à son fonctionnement.

Introduction

Contexte

3. Depuis son ouverture à la signature à Budapest, le 23 novembre 2001, la Convention sur la cybercriminalité (STE no 185 ; ci-après « la Convention ») est devenue un instrument auquel ont adhéré des pays de toutes les régions du monde et qui a un impact sur chacune d'entre elles.
4. En 2003, la Convention a été complétée par le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE no 189 ; ci-après le « Premier Protocole »).
5. Les technologies de l'information et des communications ont évolué et transformé de façon extraordinaire la société partout dans le monde depuis l'ouverture de la Convention à la signature en 2001. Toutefois, depuis lors, on a également constaté une augmentation significative de l'exploitation de technologies à des fins criminelles. La cybercriminalité est désormais considérée par de nombreuses Parties comme une grave menace pour les droits de l'homme, l'État de droit et le fonctionnement des sociétés démocratiques. Les menaces posées par la cybercriminalité sont nombreuses. On peut citer comme exemple la violence sexuelle exercée en ligne contre des enfants et les autres atteintes à la dignité et à l'intégrité des personnes ; le vol et l'utilisation abusive de données personnelles qui constituent une ingérence dans le droit au respect de la vie privée ; l'ingérence dans les processus électoraux et autres attaques contre les institutions démocratiques ;

les attaques contre les infrastructures critiques telles que celles exercées par déni de service distribué et par des logiciels rançonneurs ; ou l'utilisation abusive de ces technologies à des fins terroristes. En 2020 et en 2021, pendant la pandémie de covid-19, les pays ont observé une importante cybercriminalité liée au covid-19, qui a pris des formes variées: attaques contre les hôpitaux et établissements médicaux qui développent des vaccins contre le virus, utilisation abusive de noms de domaine pour promouvoir de faux vaccins, traitements et remèdes, ainsi que d'autres types d'activités frauduleuses.

6. Malgré la croissance des technologies fondées sur les données et l'expansion et l'évolution pernicieuses de la cybercriminalité, les concepts énoncés dans la Convention sont neutres sur le plan technologique, de sorte que le droit pénal matériel peut être appliqué aux technologies concernées tant actuelles que futures, et la Convention reste essentielle dans la lutte contre la cybercriminalité. La Convention vise principalement à: (i) harmoniser les éléments de droit pénal matériel interne des infractions et les dispositions connexes dans le domaine de la cybercriminalité ; (ii) prévoir les procédures pénales internes nécessaires pour les enquêtes et les poursuites concernant ces infractions ainsi que d'autres infractions commises au moyen d'un système informatique ou relatives à l'utilisation de preuves électroniques d'autres infractions ; et (iii) mettre en place des mécanismes rapides et efficaces de coopération internationale.

7. En appliquant la Convention, les Parties respectent la responsabilité qu'ont les gouvernements de protéger les individus contre la criminalité, qu'elle soit commise en ligne ou hors ligne, par des enquêtes et des poursuites pénales efficaces. En effet, certaines Parties à la Convention considèrent qu'elles sont liées par une obligation internationale de fournir les moyens de protection contre les infractions commises au moyen d'un système informatique (voir *K.U. c. Finlande*, Cour européenne des droits de l'homme (Requête no 2872/02, jugement/décision du 2 mars 2009) (qui fait référence aux procédures et pouvoirs en matière d'enquêtes ou de procédures pénales que les Parties doivent établir en vertu de la Convention)).

8. Les Parties ont constamment cherché à remplir leur engagement de lutter contre la cybercriminalité en s'appuyant sur divers mécanismes et organes créés en vertu de la Convention et en prenant les mesures nécessaires pour permettre des enquêtes et des procédures pénales plus efficaces. Il est important de noter que l'utilisation et la mise en œuvre de la Convention sont facilitées par le Comité de la Convention sur la cybercriminalité (T-CY)

établi en vertu de l'article 46 de cette Convention. En outre, la Convention est soutenue par des programmes de renforcement des capacités mis en œuvre par le Bureau du programme sur la cybercriminalité du Conseil de l'Europe à Bucarest, en Roumanie, qui aident les pays du monde entier à appliquer la Convention. Ce triangle composé (i) des normes communes de la Convention dans le domaine de la cybercriminalité, associé (ii) à un mécanisme solide d'engagement permanent des Parties par le biais de la T-CY, et (iii) à l'accent mis sur les programmes de renforcement des capacités, a contribué de manière significative à la portée et à l'impact de la Convention.

9. En 2012, le T-CY, agissant conformément au mandat que lui confère l'article 46, paragraphe 1, de la Convention concernant « l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique » et « l'examen de l'éventualité de compléter ou d'amender la Convention », a créé le Groupe ad hoc sur l'accès frontalier aux données et sur les questions de compétence territoriale (« Groupe sur l'accès transfrontalier »). En décembre 2014, le T-CY a également terminé une évaluation des dispositions d'entraide de la Convention sur la cybercriminalité et avait adopté une série de recommandations, dont certaines devaient être traitées dans un nouveau protocole à la Convention. Ces efforts ont mené à la création, en 2015, du Groupe de travail sur l'accès de la justice pénale aux preuves stockées dans le « nuage », y compris par le biais de l'entraide judiciaire (« Groupe sur les preuves dans le nuage »).

10. En 2016, le Groupe sur les preuves dans le nuage a conclu, entre autres points, que « la cybercriminalité, le nombre de terminaux, de services et d'utilisateurs (notamment de terminaux et services mobiles) et, partant, le nombre de victimes ont atteint des proportions telles que seule une infime partie de la cybercriminalité ou autres infractions impliquant des preuves électroniques sera jamais enregistrée et donnera jamais lieu à des enquêtes. L'immense majorité des victimes ne peut pas s'attendre à ce que justice soit rendue. Les principales difficultés mises en évidence par le groupe concernaient « l'informatique en nuage, la territorialité et la compétence » et, de ce fait, la difficulté d'obtention d'un accès efficace aux preuves électroniques et leur divulgation.

11. En examinant les conclusions du Groupe sur les preuves dans le nuage, les Parties à la Convention ont conclu qu'il n'était pas nécessaire de modifier la Convention ni de prévoir de nouvelles incriminations par le biais du droit

pénal matériel. Toutefois, les Parties sont convenues que des mesures supplémentaires devaient être prises pour renforcer la coopération et la capacité des autorités de justice pénale à obtenir des preuves électroniques en élaborant un deuxième protocole additionnel, ce afin de rendre plus efficace l'action de la justice pénale et de préserver l'État de droit.

Les travaux préparatoires

12. Lors de sa 17^e réunion plénière (8 juin 2017), le T-CY a approuvé le mandat pour la préparation du présent Protocole sur la base d'une proposition formulée par le Groupe sur les preuves dans le nuage. Il a décidé d'engager de sa propre initiative le processus de rédaction de ce Protocole en se prévalant de l'article 46, paragraphe 1.c, de la Convention. Le 14 juin 2017, la Secrétaire Générale adjointe du Conseil de l'Europe a informé le Comité des Ministres (lors de la 1289^e réunion des Délégués des Ministres) de cette initiative du T-CY.

13. Couvrant initialement la période allant de septembre 2017 à décembre 2019, le mandat a été ultérieurement prorogé par le T-CY jusqu'en décembre 2020, puis à nouveau jusqu'en mai 2021.

14. En application des dispositions de ce mandat, le T-CY a créé une réunion plénière de rédaction du Protocole (PDP) composée de représentants des Parties à la Convention, et d'États, d'organisations et d'organes du Conseil de l'Europe dotés du statut d'observateur auprès du T-CY en qualité d'observateurs. La PDP était assistée dans la préparation du projet de protocole d'un Groupe de rédaction du Protocole (PDG), composé d'experts des Parties à la Convention. Le PDG a créé à son tour plusieurs sous-groupes et groupes ad hoc chargés d'élaborer des dispositions spécifiques.

15. Entre septembre 2017 et mai 2021, le T-CY a tenu 10 Plénières de rédaction, 16 réunions du groupe de rédaction et un grand nombre de réunions de sous-groupe et de groupe ad hoc. La plus grande partie du présent Protocole a été préparée pendant la pandémie de covid-19. Du fait des restrictions liées à la covid-19, entre mars 2020 et mai 2021, plus de 65 réunions ont eu lieu par visioconférence.

16. Les méthodes de travail susvisées (plénières, groupes de rédaction et sous-groupes et groupes ad hoc) ont permis aux représentants et aux experts des Parties d'apporter des contributions très importantes à la rédaction du Protocole et de mettre au point des solutions innovantes.

17. La Commission de l'Union européenne a participé à ces travaux au nom des États parties à la Convention qui étaient membres de l'Union européenne en vertu d'un mandat de négociation conféré par le Conseil de l'Union européenne le 6 juin 2019.

18. Une fois le projet de dispositions établi et adopté à titre provisoire par le PDP, ce projet d'articles a été publié et les parties prenantes ont été invitées à formuler des observations à son sujet.

19. Le T-CY a organisé six séries de consultations avec les parties prenantes de la société civile et du secteur privé ainsi que des experts en protection des données: en marge de la Conférence Octopus sur la cybercriminalité à Strasbourg en juillet 2018, avec des experts en protection des données à Strasbourg en novembre 2018, sous la forme d'une invitation à présenter des observations écrites sur le projet d'articles en février 2019, en marge de la Conférence Octopus sur la cybercriminalité à Strasbourg en novembre 2019, sous la forme d'une invitation à présenter des observations écrites sur le nouveau projet d'articles en décembre 2020, et en mai 2021 via des soumissions écrites et une réunion virtuelle tenue le 6 mai 2021.

20. Par ailleurs, le T-CY a consulté le Comité européen pour les problèmes criminels (CDPC) 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) du Conseil de l'Europe.

21. La 24e plénière du T-CY tenue le 28 mai 2021 a approuvé le projet du présent Protocole et a décidé de le soumettre au Comité des Ministres pour adoption.

Questions de fond

22. Du point de vue du fond, les travaux d'élaboration du présent Protocole sont partis, d'une part, des résultats de l'évaluation par le T-CY, en 2014, des dispositions de la Convention relatives à l'entraide, ainsi que des analyses et recommandations du Groupe sur l'accès transfrontalier et du Groupe sur les preuves dans le nuage, en 2014 et 2017, respectivement. En particulier, les défis en matière de territorialité et de compétence se rapportant aux preuves électroniques, c'est-à-dire le fait que les données nécessaires aux fins d'une enquête pénale peuvent être stockées dans des juridictions multiples, changeantes ou inconnues (« dans le nuage »), et le fait que des solutions doivent être apportées pour obtenir la divulgation de ces données de façon efficace et efficiente aux fins d'enquêtes ou de procédures pénales données, ont été jugés préoccupants.

23. Devant la complexité de ces défis, les rédacteurs du présent Protocole sont convenus d'axer leur attention sur les questions spécifiques énumérées ci-après:

- au moment de la rédaction du Protocole, les demandes d'entraide étaient la principale méthode pour obtenir des preuves électroniques d'une infraction pénale auprès d'autres États, y compris les outils d'entraide de la convention. Toutefois, l'entraide n'est pas toujours un bon moyen de traiter un nombre croissant de demandes de preuves électroniques volatiles. On a donc jugé nécessaire de mettre au point un mécanisme plus simple pour émettre des ordres ou des demandes aux fournisseurs de services d'autres parties afin de produire des informations sur les abonnés et des données relatives au trafic ;
- les données relatives aux abonnés – servant par exemple à identifier l'utilisateur d'un compte de messagerie électronique ou de média social, ou d'une adresse IP (internet protocol) utilisée pour commettre une infraction – sont les données le plus souvent recherchées dans les enquêtes pénales nationales et internationales liées à la cybercriminalité et à d'autres crimes impliquant des preuves électroniques. En l'absence de ces données, il est souvent impossible de poursuivre une enquête. Dans la plupart des cas, le recours à l'entraide judiciaire pour obtenir les données relatives aux abonnés n'est pas efficace et engorge le système d'entraide judiciaire. Ces données sont d'ordinaire détenues par les fournisseurs de services. L'article 18 de la Convention traite bien certains aspects de l'obtention des données relatives aux abonnés auprès des fournisseurs de services (voir la note d'orientation du T-CY relative à l'article 18), y compris dans les autres Parties, mais il a été jugé nécessaire de concevoir des outils complémentaires pour obtenir la divulgation de données relatives aux abonnés directement auprès d'un fournisseur de services d'une autre Partie. Ces outils permettraient d'accroître l'efficacité du processus et aussi d'alléger la pression sur le système d'entraide ;
- les données relatives au trafic sont également souvent recherchées dans le cadre d'enquêtes criminelles, et leur divulgation rapide peut s'avérer nécessaire pour remonter à la source d'une communication et servir de point de départ à la collecte de preuves supplémentaires ou à l'identification d'un suspect ;
- de même, comme de nombreuses formes de criminalité en ligne sont facilitées par des domaines créés ou exploités à des fins criminelles, il est nécessaire d'identifier la personne qui a enregistré un domaine de ce

type. De telles informations sont détenues par des entités fournissant des services d'enregistrement de noms de domaine, c'est-à-dire, en général, des registraires et des registres. Il s'impose donc de mettre en place un dispositif efficace permettant d'obtenir ces informations auprès des entités en question dans les autres Parties ;

- lorsque, dans une situation d'urgence, il existe un risque grave et imminent pour la vie ou la sécurité d'une personne physique, il faut intervenir rapidement soit en fournissant une entraide d'urgence, soit en utilisant le réseau de points de contact disponibles 24 heures sur 24 créé en application de la Convention (article 35) ;
- en outre, les outils éprouvés de coopération internationale devraient être utilisés plus largement et entre toutes les parties. D'importantes mesures telles que la visioconférence ou les équipes communes d'enquête sont d'ores et déjà disponibles en vertu d'instruments du Conseil de l'Europe (par exemple, le Deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, STE no 182, ci-après le « Deuxième Protocole STE no 182 ») ou d'autres accords bilatéraux et multilatéraux. Cependant, de tels mécanismes ne sont pas universellement disponibles parmi les Parties à la Convention, et le Protocole vise à combler cette lacune ;
- la Convention prévoit la collecte et l'échange d'informations et de preuves pour des enquêtes ou des procédures pénales spécifiques. Les rédacteurs ont reconnu que l'établissement, la mise en œuvre et l'application des pouvoirs et des procédures liés aux enquêtes et aux poursuites pénales devaient toujours être soumis à des conditions et à des garanties qui assurent une protection adéquate des droits de l'homme et des libertés fondamentales. Il était donc nécessaire d'inclure un article sur les conditions et les garanties (analogue à l'article 15 de la Convention). En outre, reconnaissant l'exigence de nombreuses Parties de protéger la vie privée et les données à caractère personnel afin de satisfaire à leurs obligations constitutionnelles et internationales, les rédacteurs ont décidé de prévoir des garanties spécifiques de protection des données dans ce Protocole. Ces garanties de protection des données complètent les obligations de nombreuses Parties à la Convention, qui sont également parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE no 108). Le protocole d'amendement à cette convention (STCE no 223) a été ouvert à la signature lors de la rédaction du présent Protocole en octobre 2018. Il convient également de noter que le

processus de rédaction de ce Protocole a associé des Parties non soumises, à l'époque, aux instruments du Conseil de l'Europe relatifs à la protection des données ni aux règles de protection des données de l'Union européenne. En conséquence, des efforts importants ont été consentis pour élaborer un Protocole équilibré qui tienne compte des nombreux systèmes juridiques des États appelés à devenir parties au Protocole tout en notant qu'il importait d'assurer la protection de la vie privée et à la protection des données comme l'exigent les constitutions et les obligations internationales des autres Parties à la Convention.

24. Les rédacteurs ont également examiné d'autres mesures qui, à l'issue d'une discussion approfondie, n'ont pas été retenues dans le présent Protocole. Deux de ces dispositions, à savoir les « enquêtes clandestines à l'aide d'un système informatique » et l'« extension du champ des perquisitions », présentaient un grand intérêt pour les Parties, mais auraient exigé des efforts, du temps supplémentaires et de nouvelles consultations avec les parties prenantes. Il n'a donc pas été jugé possible de les traiter dans le délai imparti pour la préparation du présent Protocole. Les rédacteurs ont proposé d'en poursuivre l'examen sous une autre forme et, éventuellement, dans le cadre d'un instrument juridique distinct.

25. Dans l'ensemble, les rédacteurs ont considéré que les dispositions du présent Protocole apporteraient une forte valeur ajoutée sur le plan opérationnel aussi bien que sur celui des principes directeurs. Le Protocole améliorera considérablement la capacité des Parties à renforcer la coopération entre les Parties et entre les Parties et les fournisseurs de services et autres entités, et à obtenir la divulgation de preuves électroniques aux fins d'enquêtes ou de procédures pénales spécifiques. Ainsi, ce Protocole, comme la Convention, vise à accroître la capacité des autorités de justice pénale à lutter contre la cybercriminalité et d'autres infractions, tout en respectant pleinement les droits de l'homme et les libertés fondamentales, et il souligne l'importance et la valeur d'un internet fondé sur la libre circulation des informations.

Le Protocole

26. Comme cela est énoncé dans le préambule, le présent Protocole vise à renforcer davantage la coopération en matière de cybercriminalité, et la capacité des autorités de justice pénale à recueillir des preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques au moyen d'outils supplémentaires ayant trait à une

entraide judiciaire plus efficace et à d'autres formes de coopération entre autorités compétentes ; la coopération dans les situations d'urgence (c'est-à-dire les situations où existe un risque important et imminent pour la vie ou la sécurité d'une personne physique) et la coopération directe entre les autorités compétentes et les fournisseurs de services et d'autres entités ayant en leur possession ou sous leur contrôle des informations pertinentes. Le présent Protocole a donc pour but de compléter la Convention et, entre les Parties à celle-ci, le Premier Protocole.

27. Le présent Protocole est divisé en quatre chapitres: I. Dispositions communes ; II. Mesures de coopération renforcée ; III. Conditions et garanties ; et IV. Dispositions finales.

28. Les dispositions communes du chapitre I portent sur le but et la portée de ce Protocole. Comme c'est le cas de la Convention, le Protocole a traité des enquêtes ou procédures pénales spécifiques concernant non seulement la cybercriminalité, mais toute infraction pénale pour laquelle les preuves se présentent sous forme électronique, également appelée communément « preuve électronique » ou « preuve numérique ». Ce chapitre rend les définitions de la Convention applicables au présent Protocole et donne des définitions supplémentaires pour les termes qui reviennent fréquemment dans le Protocole. De plus, étant donné que les exigences en matière de connaissance de la langue au titre de l'entraide judiciaire et d'autres formes de coopération entravent souvent l'efficacité des procédures, un article sur la « langue » a été ajouté pour permettre d'adopter une approche plus pragmatique à cet égard.

29. Le chapitre II comprend les principaux articles de fond du Protocole, qui décrivent plusieurs types de coopération disponibles pour les Parties, auxquels s'appliquent différents principes. Aussi a-t-il été nécessaire de diviser ce chapitre en sections, intitulées respectivement: 1. Principes généraux applicables au chapitre II ; 2. Procédures renforçant la coopération directe avec les fournisseurs et les entités dans les autres Parties ; 3. Procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées ; 4. Procédures relatives à la demande d'entraide urgente ; et 5. Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables.

30. Le chapitre III prévoit des conditions et des garanties. Celles-ci exigent des Parties qu'elles appliquent également des conditions et garanties analogues à celles qui font l'objet de l'article 15 de la Convention aux pouvoirs et procédures énoncés dans le présent Protocole. En outre, ce chapitre inclut

un ensemble détaillé de garanties applicables à la protection des données à caractère personnel.

31. La plupart des dispositions finales du chapitre IV sont analogues aux dispositions finales classiques des instruments du Conseil de l'Europe ou rendent les dispositions de la Convention applicables au présent Protocole. Cependant, font exception l'article 15 intitulé « Effets de ce Protocole », l'article 17 sur la « Clause fédérale » et l'article 23 intitulé « Concertation des Parties et évaluation de l'application », qui diffèrent à des degrés divers des dispositions analogues de la Convention. Non seulement ce dernier article rend l'article 46 de la Convention applicable, mais il dispose également que l'application et l'utilisation effective des dispositions du présent Protocole sont évaluées périodiquement par les Parties.

Commentaire sur les articles du Protocole

Chapitre I – Dispositions communes

Article 1 – But

32. Le présent Protocole a pour objet de compléter (i) la Convention entre les Parties au présent Protocole et (ii) le Premier Protocole entre les Parties à celui-ci qui sont également parties au présent Protocole.

Article 2 – Champ d'application

33. La portée générale d'application de ce Protocole est la même que celle de la Convention: les mesures prévues par ce Protocole doivent être appliquées, entre les Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques, concernant des infractions pénales liées à des systèmes et données informatiques (autrement dit les infractions couvertes par l'article 14 paragraphe 2.a et b, de la Convention), ainsi qu'au recueil de preuves sous forme électronique d'une infraction pénale (article 14, paragraphe 2.c, de la Convention). Comme cela est expliqué aux paragraphes 141 et 243 du rapport explicatif de la Convention, cela veut dire que, lorsque l'infraction est commise par le biais d'un système informatique, ou lorsqu'une infraction qui n'a pas été commise par le biais d'un système informatique (par exemple un meurtre) implique des preuves électroniques, les pouvoirs, procédures et mesures de coopération créées par ce Protocole ont pour finalité de pouvoir être utilisées.

34. Le paragraphe 1.b prévoit qu'entre les Parties au Premier Protocole qui sont parties à ce Protocole ce dernier s'applique aussi à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole. Les Parties à ce Protocole qui ne sont pas parties au Premier Protocole ne prennent aucun engagement les obligeant à appliquer les termes du présent Protocole à ces infractions.

35. En vertu du paragraphe 2, il est demandé à chaque Partie de disposer d'un fondement juridique pour s'acquitter des obligations prévues dans le Protocole si ses traités, droits ou dispositifs ne contiennent pas déjà ces dispositions. Cela ne fait pas de dispositions explicitement discrétionnaires des dispositions contraignantes, et certaines dispositions prévoient des déclarations et des réserves. Certaines Parties peuvent ne pas avoir besoin de textes législatifs d'application pour mettre en œuvre les dispositions de ce Protocole.

Article 3 – Définitions

36. Le paragraphe 1 reprend les définitions fournies à l'article 1 (« Système informatique », « Données informatiques », « Fournisseur de services » et « Données relatives au trafic ») et à l'article 18, paragraphe 3 (« Données relatives aux abonnés »), de la Convention dans le présent Protocole. Les rédacteurs ont repris ces définitions de la Convention parce que ces termes sont utilisés dans le dispositif et le rapport explicatif de ce Protocole. Les rédacteurs ont également prévu que les explications fournies dans le rapport explicatif de la Convention et les notes d'orientation adoptés par le T-CY au sujet de ces termes s'appliqueraient également au présent Protocole.

37. Les définitions des infractions et des autres termes utilisés dans le texte de la Convention sont destinées à s'appliquer aux fins de la coopération entre les Parties au présent Protocole, et les définitions des infractions et des autres termes utilisés dans le texte du Premier Protocole sont destinées à s'appliquer aux fins de la coopération entre les Parties au Premier Protocole. Par exemple, l'article 2, paragraphe 1, dispose que « les mesures que le présent Protocole énonce s'appliquent [...] pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques ». Par conséquent, lorsque la coopération au titre du présent Protocole porte sur des infractions liées à la pornographie infantile, la définition de la « pornographie infantile » figurant à l'article 9, paragraphe 2, de la Convention s'applique, ainsi que la définition de « mineur » figurant à l'article 9, paragraphe 3, de la Convention. De même, pour ce qui concerne

les Parties au Premier Protocole qui sont parties au présent Protocole, la définition du « matériel raciste et xénophobe » de l'article 2 du Premier Protocole s'applique. Les Parties au présent Protocole qui ne sont pas Parties au Premier Protocole ne sont pas tenues d'appliquer les termes ou définitions énoncés dans le Premier Protocole.

38. Le paragraphe 2 de l'article 3 comprend des définitions supplémentaires qui s'appliquent à ce protocole et à la coopération au titre du protocole. Le paragraphe 2.a définit l'« autorité centrale » comme étant « l'autorité ou les autorités désignées en vertu d'un traité d'entraide ou d'un arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, ou, à défaut, l'autorité ou les autorités désignées par une Partie aux termes de l'article 27, paragraphe 2.a, de la Convention ». Le Protocole utilise les autorités centrales dans plusieurs articles pour que la coopération soit assurée par un moyen que les Parties mettent déjà en œuvre et qu'elles connaissent bien. Ainsi, les Parties qui ont conclu des traités d'entraide ou des arrangements reposant sur des législations uniformes ou réciproques sont tenues d'utiliser les autorités centrales désignées aux termes de ces traités ou arrangements. Lorsque aucun traité ou arrangement de ce type n'est en vigueur entre les Parties concernées, ces dernières sont tenues d'utiliser la même autorité centrale qu'elles utilisent actuellement en vertu des dispositions de l'article 27, paragraphe 2.a, de la Convention. Tous les traités d'entraide ou arrangements reposant sur des législations uniformes ou réciproques n'utilisent pas l'expression « autorité centrale », mais les rédacteurs ont souhaité que cette dernière désigne les autorités de coordination désignées dans lesdits traités ou arrangements, quelle que soit la façon dont elles y sont dénommées.

39. Sauf disposition expresse du présent Protocole, le fait que les Parties mobilisent aux fins de ce dernier des autorités centrales ne veut pas dire que d'autres dispositions de ces traités ou arrangements d'entraide s'appliquent.

40. La définition de l'« autorité compétente » énoncée au paragraphe 2.b est inspirée du paragraphe 138 du rapport explicatif de la Convention. Le présent Protocole utilisant fréquemment cette expression, cette définition a été insérée dans le dispositif pour en faciliter la consultation.

41. Le paragraphe 2.c définit l'« urgence » comme « une situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique ». Ce terme est utilisé dans les articles 9, 10 et 12. Dans le présent Protocole, la définition de l'« urgence » est destinée à imposer un seuil nettement plus élevé que les « cas d'urgence » visés à l'article 25, paragraphe 3,

de la Convention. Par ailleurs, cette définition a été élaborée de façon que les Parties puissent prendre en considération les différents contextes dans lesquels le terme est utilisé dans le présent Protocole tout en tenant compte des lois et politiques applicables dans chacune d'elles.

42. La définition d'une urgence se rapporte aux situations dans lesquelles le risque est grave et imminent, excluant ainsi les situations dans lesquelles le risque pour la vie ou la sécurité d'une personne appartient déjà au passé ou est négligeable, ou dans lesquelles peut exister un risque futur qui n'est pas imminent. Ces prescriptions relatives à la gravité et au caractère imminent tiennent au fait que les articles 9 et 10 imposent à la Partie requise comme à la Partie requérante des obligations à forte intensité de main d'œuvre pour réagir de manière très accélérée en situation d'urgence, les demandes en urgence devant alors se voir accorder un rang de priorité plus élevé que d'autres cas qui, tout en étant importants, sont un peu moins urgents, même s'ils ont été soumis plus tôt. Les situations impliquant « un risque grave et imminent pour la vie ou la sécurité d'une personne physique » sont, par exemple, la prise d'otage, situation dans laquelle existe un risque crédible et imminent de décès, de blessure grave ou d'un autre préjudice comparable pour la victime ; la persistance des abus sexuels auxquels un enfant est soumis ; les scénarios immédiatement postérieurs à une attaque terroriste, dans lesquels les autorités cherchent à savoir avec qui les attaquants ont été en communication afin de déterminer si de nouvelles attaques sont imminentes, et les menaces pour la sécurité d'infrastructures essentielles s'accompagnant d'un risque grave et imminent pour la vie ou la sécurité d'une personne physique.

43. Comme cela est expliqué à l'article 10, paragraphe 4, du Protocole et au paragraphe 154 du présent rapport explicatif qui concerne l'article 9, une Partie requise déterminera, en vertu de ces articles, si une « urgence » existe, en appliquant la définition donnée dans le présent article.

44. Le paragraphe 2.d définit les « données à caractère personnel » comme « les informations relatives à une personne physique identifiée ou identifiable ». On entend par « personne physique identifiable » une personne qui peut être identifiée, directement ou indirectement, à partir, en particulier, d'un numéro d'identification ou d'un ou plusieurs facteurs propres à son identité physique, physiologique, mentale, économique, culturelle ou sociale. La définition des « données à caractère personnel » dans le présent Protocole correspond à celle donnée par d'autres instruments internationaux, comme la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel telle que modifiée par son Protocole d'amendement, les

Lignes directrices de 2013 de l'Organisation de coopération et de développement économiques sur la protection de la vie privée et les flux transfrontières de données à caractère personnel, le Règlement général de protection des données et la directive de l'Union européenne en matière de protection des données dans le domaine répressif, ainsi que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (« Convention de Malabo »).

45. Une personne n'est pas considérée comme « identifiable » lorsque l'identification nécessiterait un temps, des efforts ou des ressources déraisonnables. Si certaines informations sont propres à une personne donnée et établissent donc par définition un lien avec cette personne, d'autres informations peuvent ne permettre une identification qu'en combinaison avec des informations identifiantes ou à caractère personnel supplémentaires. En conséquence, si l'identification d'une personne par recoupement avec des informations supplémentaires de cette nature devait nécessiter un temps, des efforts ou des ressources déraisonnables, les informations dont il est question ne constituent pas des données à caractère personnel. Le fait qu'une personne physique puisse être identifiée ou soit identifiable, directement ou indirectement, dépend des circonstances propres à un contexte donné (et peut varier dans le temps avec les innovations technologiques ou autres).

46. Les exigences de protection des données fixées par le présent Protocole ne s'appliquent pas aux données qui n'ont pas de « caractère personnel », comme les informations anonymisées qui ne peuvent pas être réidentifiées sans y consacrer un temps, des efforts ou des ressources déraisonnables.

Article 4 – Langue

47. L'article 4 fournit un cadre pour les langues qui peuvent être utilisées lorsque l'on s'adresse aux Parties et aux fournisseurs de services ou autres entités en vertu du présent Protocole. Même lorsque, dans la pratique, les Parties sont en mesure de travailler dans des langues autres que leurs langues officielles, cette possibilité peut ne pas être prévue par le droit interne ou les traités. L'objectif de cet article est d'apporter plus de souplesse dans le cadre du présent Protocole.

48. Les traductions inexactes ou coûteuses des demandes d'entraide en matière de preuves électroniques sont constamment critiquées et constituent un problème qui doit être traité d'urgence. Cet obstacle sape les processus légitimes d'obtention de données et de protection de la sécurité publique.

Les mêmes considérations s'appliquent en dehors de l'entraide judiciaire traditionnelle, par exemple lorsqu'une Partie transmet une injonction directement à un fournisseur de services sur le territoire d'une autre Partie en vertu de l'article 7, ou demande de donner effet à une injonction en vertu de l'article 8. Les possibilités de traduction automatique devraient s'améliorer, mais elles sont actuellement insuffisantes. Pour ces raisons, le problème de la traduction a été mentionné à plusieurs reprises dans les propositions relatives aux articles à inclure dans ce Protocole.

49. La traduction de et vers des langues moins courantes est particulièrement problématique, car ces traductions peuvent retarder considérablement une demande ou être dans les faits impossibles à obtenir. Elles peuvent aussi être extrêmement trompeuses et leur mauvaise qualité peut faire perdre du temps aux deux Parties. Toutefois, le coût et la difficulté des traductions incombent de manière disproportionnée aux Parties requérantes où des langues moins courantes sont parlées.

50. En raison de cette charge disproportionnée, un certain nombre de Parties non anglophones ont demandé que l'anglais soit obligatoire dans ce Protocole. Ils ont noté que l'anglais était une langue couramment utilisée par les principaux fournisseurs de services. En outre, à mesure que les données sont déplacées et stockées plus largement dans le monde et que de plus en plus de pays s'entraident, la traduction peut devenir encore plus lourde et peu pratique. Par exemple, deux Parties peuvent utiliser des langues moins courantes, être géographiquement éloignées et avoir peu de contacts. Si la Partie A a soudainement besoin de l'aide de la Partie B, il se peut qu'elle ne parvienne pas à trouver un traducteur pour la langue de la Partie B, ou qu'une traduction éventuelle soit moins intelligible que la traduction anglaise effectuée par des personnes non anglophones. Les rédacteurs ont particulièrement souligné que, pour accélérer l'assistance, tous les efforts devraient être faits pour accepter, en particulier, les demandes d'urgence au titre du présent Protocole, en anglais ou dans une langue commune, plutôt que d'exiger une traduction dans la langue officielle de la Partie requise.

51. Les rédacteurs du Protocole ont conclu que l'anglais ne devrait pas être obligatoire dans le texte de ce Protocole. Certaines Parties ont des exigences en matière de langues officielles qui excluent un tel mandat ; de nombreuses Parties partagent une langue commune et n'ont pas besoin de l'anglais ; et, dans certaines Parties, les fonctionnaires en dehors des capitales sont moins susceptibles de pouvoir lire l'anglais mais sont souvent impliqués dans l'exécution des demandes.

52. Ainsi, le paragraphe 1 est formulé en termes de « langue acceptable pour la Partie requise ou la Partie à laquelle les actes sont notifiés en vertu de l'article 7 ». Cette Partie peut spécifier des langues acceptables – par exemple des langues largement répandues comme l'anglais, l'espagnol ou le français – même si elles ne sont pas prévues dans sa législation ou ses traités nationaux.

53. Au paragraphe 1, les termes « demandes, injonctions et renseignements qui les accompagnent » désignent:

- en vertu de l'article 8, la demande (paragraphe 3), l'injonction (paragraphe 3.a), des renseignements à l'appui (paragraphe 3.b) et de toute instruction spéciale de procédure (paragraphe 3.c) ;
- dans le cas des Parties qui exigent une notification en vertu de l'article 7, paragraphe 5, l'injonction (paragraphe 3), les renseignements à l'appui (paragraphe 4) et le résumé des faits (paragraphe 5.a) ;
- en vertu de l'article 9, la requête (paragraphe 3).

Le terme « demandes » renvoie également au contenu des demandes en vertu des articles 10, 11 et 12, qui comprend la documentation qui fait partie de la demande.

54. Dans la pratique, certains pays peuvent être disposés à accepter des demandes et des injonctions dans une langue autre qu'une langue spécifiée dans le droit interne ou dans les traités. Aussi, une fois par an, le T-CY mènera une enquête informelle sur les langues acceptables pour les demandes et les injonctions. Les Parties peuvent modifier leurs renseignements en tout temps et l'ensemble des Parties seront informées de ces changements. Elles peuvent indiquer qu'elles n'acceptent que des langues spécifiques pour certaines formes d'assistance. Les résultats de cette enquête seront visibles pour toutes les Parties à la Convention, et pas seulement pour les Parties à ce Protocole.

55. Cette disposition pragmatique démontre l'extrême importance d'accélérer la coopération. Elle fournit une base conventionnelle permettant à une Partie d'accepter d'autres langues aux fins du présent Protocole.

56. Dans de nombreux cas, les Parties ont conclu des traités d'entraide judiciaire qui précisent la ou les langues dans lesquelles les demandes doivent être présentées en vertu de ces traités. Le présent article n'interfère pas avec les termes de ces traités ou autres accords entre les Parties. En outre, aux fins du présent Protocole, on s'attend à ce qu'« une langue acceptable pour la Partie requise ou la Partie à laquelle les actes sont notifiés en vertu de l'article 7 »

comprenne toute langue ou toutes langues spécifiées par ces traités ou accords. Par conséquent, une Partie requérante devrait appliquer la langue spécifiée dans les traités d'entraide judiciaire ou autres accords aux demandes et notifications faites au titre du présent Protocole, à moins que la Partie requise ou à laquelle les actes sont notifiés n'indique qu'elle est également disposée à accepter ces demandes ou notifications dans d'autres langues.

57. Si une Partie est disposée à accepter d'autres langues, elle indiquera au T-CY qu'elle a l'intention d'accepter certaines ou toutes sortes de demandes ou de notifications d'injonctions au titre du présent Protocole dans une autre langue.

58. Le paragraphe 2 détermine la(les) langue(s) que la Partie émettrice utilise pour soumettre des injonctions ou des demandes et les renseignements connexes aux fournisseurs de services ou des entités fournissant des services d'enregistrement de noms de domaine sur le territoire d'une autre Partie conformément aux articles 7 et 6 respectivement. Cette disposition vise à assurer une coopération rapide et une certitude accrue sans imposer une charge supplémentaire aux fournisseurs de services ou des entités lorsqu'ils reçoivent des injonctions ou des demandes de données. La première option prévue au paragraphe 2.a indique que l'injonction ou la demande peut être présentée dans une langue dans laquelle le fournisseur de services ou l'entité accepte habituellement des injonctions ou demandes nationales de ses propres autorités dans le cadre d'enquêtes spécifiques ou de procédures pénales (« procédure interne comparable »). Pour les Parties qui ont une ou plusieurs langues officielles, il s'agirait d'une de ces langues. La deuxième option, prévue au paragraphe 2.b, indique que, si un fournisseur de services ou l'entité accepte de recevoir des injonctions ou des demandes dans une autre langue, par exemple la langue de son siège, ces injonctions et les informations qui les accompagnent peuvent être soumises dans cette langue. En tant que troisième option, le paragraphe 2.c prévoit que, lorsque l'injonction ou la demande et les informations qui l'accompagnent ne sont pas émises dans l'une des langues des deux premières options, elles sont accompagnées d'une traduction dans l'une de ces langues.

59. Au paragraphe 2, les termes « injonctions en vertu de l'article 7 et les demandes en vertu de l'article 6, et tout renseignement complémentaire » désignent:

- en vertu de l'article 6, la demande (paragraphe 3) ; et
- en vertu de l'article 7, l'ordonnance (paragraphe 3) et les informations complémentaires (paragraphe 4).

60. Lorsqu'une Partie a exigé une notification conformément à l'article 7, une Partie requérante doit être prête à envoyer l'injonction et tout renseignement qui l'accompagne dans une langue acceptable pour la Partie qui exige la notification, même si le fournisseur de services accepte d'autres langues.

61. Le T-CY s'efforcera également de recueillir de manière informelle des informations sur les langues dans lesquelles les injonctions et les demandes ainsi que les informations qui les accompagnent seront soumises aux fournisseurs de services et aux entités fournissant des services d'enregistrement de noms de domaine conformément à l'article 4, paragraphe 2, et en informera les Parties dans le cadre de l'enquête décrite au paragraphe 54 du présent rapport explicatif.

Chapitre II – Mesures de coopération renforcée

Section 1 – Principes généraux applicables au chapitre II

Article 5 – Principes généraux applicables au chapitre II

62. Le paragraphe 1 de l'article 5 précise que les Parties s'assurent la coopération « la plus large possible », conformément aux dispositions du chapitre II et comme prévu à l'article 23 et à l'article 25, paragraphe 1, de la Convention. Ce principe fait obligation aux Parties de s'assurer une coopération étendue et de réduire au minimum les obstacles à la circulation rapide et fluide de l'information et des preuves entre pays.

63. Les paragraphes 2 à 5 organisent les sept mesures de coopération du présent Protocole en quatre sections distinctes qui suivent la première section, relative aux principes généraux. Ces sections portent sur les différents types de coopération visés: la section 2 couvre la coopération directe avec des entités privées, la section 3 concerne la coopération renforcée entre les autorités pour la divulgation de données stockées, la section 4 porte sur l'entraide en cas d'urgence et la section 5 conclut par les dispositions internationales régissant la coopération en l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées. Ces sections sont aussi structurées de manière globalement progressive, allant des formes d'assistance souvent souhaitées dans les premiers stades d'une enquête – pour obtenir la divulgation de l'enregistrement de noms de domaine et informations relatives aux abonnés – aux demandes de données relatives au trafic puis aux données

relatives au contenu, suivies des vidéoconférences et des équipes communes d'enquête, qui sont souvent les formes d'assistance recherchées à un stade plus avancée d'une enquête.

64. Cette section consacrée aux principes généraux indique clairement à quel point chaque mesure est affectée ou non par l'existence d'un traité d'entraide ou d'un arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, c'est-à-dire entre la Partie requérante et la Partie requise dans le cas de la coopération interétatique ou la Partie demandant les informations et la Partie sur le territoire de laquelle est située l'entité privée qui est en possession de ces informations ou qui en a le contrôle, pour la coopération directe en vertu des articles 6 et 7. On entend par « arrangement sur la base de législations uniformes ou réciproques » les mécanismes « tels que le système de coopération instauré entre les pays nordiques, qui est également reconnu par la Convention européenne d'entraide judiciaire en matière pénale (article 25, paragraphe 4), et le système instauré entre les membres du Commonwealth » (voir le paragraphe 263 du rapport explicatif de la Convention). Les mesures prévues aux sections 2 à 4 de ce chapitre s'appliquent, que les Parties concernées soient ou non mutuellement liées par un accord d'entraide ou un arrangement applicable reposant sur des législations uniformes ou réciproques. Les dispositions de la section 5 relatives à la coopération internationale s'appliquent uniquement en l'absence d'un tel accord ou d'un tel arrangement, sauf dispositions contraires.

65. Comme cela est décrit au paragraphe 2 de l'article 5, la section 2 se compose de l'article 6, intitulé « Demande d'informations concernant l'enregistrement d'un nom de domaine », et de l'article 7, intitulé « Divulgence de données relatives aux abonnés ». Il s'agit des articles dits de « coopération directe », qui permettent aux autorités compétentes d'une Partie de s'engager directement avec des entités privées – c'est-à-dire avec des entités fournissant des services d'enregistrement de noms de domaine à l'article 6, et avec des fournisseurs de services à l'article 7 – aux fins d'enquêtes ou de procédures pénales spécifiques. L'article 2 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre la Partie qui recherche les informations et la Partie sur le territoire de laquelle se trouve l'entité privée en possession ou en charge de ces informations.

66. Comme cela est décrit au paragraphe 3 de l'article 5, la section 3 du chapitre II se compose de l'article 8, intitulé « Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux

informations sur les abonnés et au trafic », et de l'article 9, intitulé « Divulgence accélérée de données informatiques stockées en situation d'urgence ». Il s'agit de mesures de « coopération internationale renforcée entre autorités », c'est-à-dire qu'elles prévoient une coopération entre autorités compétentes, mais d'une nature différente de la coopération internationale traditionnelle. La section 3 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les parties requérante et requise.

67. Comme cela est décrit au paragraphe 4 de l'article 5, la section 4 du chapitre II se compose de l'article 10, intitulé « Entraide d'urgence ». Bien que l'entraide d'urgence soit une disposition d'entraide, elle constitue un outil de coopération important pour les situations d'urgence qui n'est pas expressément prévu dans de nombreux traités d'entraide. Par conséquent, les rédacteurs ont décidé que cette section devait s'appliquer, qu'il existe ou non un accord ou un arrangement d'entraide applicable, sur la base de la législation uniforme ou réciproque en vigueur entre les Parties concernées. En ce qui concerne les procédures qui régissent l'entraide en cas d'urgence, il existe deux possibilités. Lorsque les Parties concernées sont mutuellement liées par un accord d'entraide applicable, ou un arrangement d'entraide applicable sur la base d'une législation uniforme ou réciproque, la section 4 est complétée par les dispositions de cet accord, à moins que les Parties concernées ne décident mutuellement d'appliquer certaines dispositions de la Convention à la place (voir l'article 10, paragraphe 8). Lorsque les Parties concernées ne sont pas mutuellement liées par un tel accord ou arrangement, les Parties appliquent certaines procédures énoncées aux articles 27 et 28 de la Convention régissant l'entraide en l'absence de traité (voir l'article 10, paragraphe 7, de ce Protocole).

68. Comme cela est décrit au paragraphe 5 de l'article 5, la section 5 du chapitre II se compose de l'article 11, intitulé « Vidéoconférence », et de l'article 12, intitulé « Équipes communes d'enquête et enquêtes communes ». Ces dispositions sont des mesures de coopération internationale, qui ne s'appliquent que lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les Parties requérante et requise. Ces mesures ne s'appliquent pas lorsqu'un tel traité ou arrangement existe, mais l'article 12, paragraphe 7, s'applique qu'un tel traité ou arrangement existe ou non. Toutefois, les Parties concernées peuvent décider mutuellement d'appliquer les dispositions de la section 5 en lieu et place d'un tel traité ou arrangement existant, à moins que cela ne soit interdit par les termes du traité ou de l'arrangement.

69. Le paragraphe 6 prend pour modèle l'article 25, paragraphe 5, de la Convention, et le paragraphe 259 du rapport explicatif de la Convention est donc également valable ici : « Lorsque la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination [...], cette condition sera considérée comme satisfaite si le comportement constituant l'infraction en relation avec laquelle l'entraide est requise est également qualifié d'infraction pénale par le droit interne de la Partie requise, même si ledit droit interne classe l'infraction dans une catégorie d'infractions différente ou la désigne en utilisant une terminologie différente. Cette disposition a été jugée nécessaire afin de garantir que les parties requises ne recourent pas à un critère trop rigide lorsqu'elles appliquent la double incrimination. Étant donné les différences entre les ordres juridiques nationaux, on ne s'étonnera pas de constater des différences de terminologie et de classement des comportements criminels. Si le comportement constitue une infraction pénale dans les deux ordres juridiques, ces différences d'ordre technique ne devraient pas empêcher l'octroi de l'entraide. Dans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance. »

70. Le paragraphe 7 prévoit que « [l]es dispositions du présent chapitre ne restreignent pas la coopération entre les Parties, ou entre les Parties et les fournisseurs de services ou d'autres entités, par le biais d'autres accords, arrangements, pratiques ou le droit interne applicables. » Cela signifie que le Protocole n'élimine ni ne restreint aucune coopération entre les Parties ou entre les Parties et des entités privées, qui est par ailleurs disponible – que ce soit par le biais d'accords, d'arrangements, du droit interne applicables ou même de pratiques informelles. Les rédacteurs avaient l'intention d'élargir, et non de restreindre, les outils disponibles dans la boîte à outils du praticien de l'application des lois pour obtenir des informations ou des preuves dans le cadre d'enquêtes ou de procédures pénales spécifiques. Les rédacteurs ont reconnu que, dans certaines situations, les mécanismes existants, tels que l'entraide judiciaire, peuvent être les mieux utilisés par un praticien. Cependant, dans d'autres situations, les outils créés par ce Protocole peuvent être plus efficaces ou préférables. Par exemple, si une autorité compétente a besoin de données relatives au contenu de manière non urgente, elle choisira probablement d'utiliser une demande d'entraide traditionnelle en vertu d'un traité bilatéral ou de l'article 27 de la Convention, selon le cas, car le Protocole ne contient pas de dispositions permettant d'obtenir des données relatives au contenu de manière non urgente. Mais si elle avait besoin d'informations sur les abonnés, elle pourrait choisir d'utiliser l'article 7 du Protocole pour émettre un ordre directement à un fournisseur de services.

71. Enfin, un certain nombre de dispositions du chapitre II et d'autres dispositions du Protocole permettent d'imposer des limitations ou des conditions d'utilisation, telles que la confidentialité. Lorsque, conformément aux dispositions du Protocole, la réception des preuves ou des informations recherchées est soumise à une telle limitation ou condition d'utilisation, des exceptions ont été reconnues par les négociateurs et sont implicites dans le texte. Premièrement, en tant que mesure de protection des droits de l'homme et des libertés conformément à l'article 13, en vertu des principes juridiques fondamentaux de nombreux États, si des éléments fournis à la Partie destinataire sont considérés par celle-ci comme étant à décharge d'une personne accusée, ils doivent être divulgués à la défense ou à une autorité judiciaire. Ce principe est sans préjudice du texte de l'article 12, paragraphe 6.b, et du rapport explicatif, paragraphe 215, qui peuvent être appliqués lorsque les Parties ont mis en place une équipe commune d'enquête. Il est entendu par les rédacteurs que, dans de tels cas, la Partie destinataire avise la Partie transférante avant la divulgation et, si cette dernière le demande, consulte la Partie transférante. Deuxièmement, lorsqu'une limitation d'utilisation a été imposée à l'égard de matériel reçu en vertu du présent Protocole et dont l'utilisation est prévue au cours d'un procès, le procès (y compris les divulgations au cours des procédures judiciaires préalables au procès) est normalement une procédure publique. Une fois rendu public lors du procès, le matériel tombe dans le domaine public. Dans ces situations, il n'est pas possible de garantir la confidentialité de l'enquête ou de la procédure pour laquelle le matériel a été demandé. Ces exceptions sont analogues aux exceptions liées à l'application de l'article 28, paragraphe 2, de la Convention, comme cela est expliqué au paragraphe 278 du rapport explicatif de la Convention. Enfin, le matériel peut être utilisé à d'autres fins lorsque le consentement préalable d'une Partie transférante a été obtenu.

Section 2 – Procédures renforçant la coopération directe avec les fournisseurs et les entités des autres Parties

Article 6 – Demande d'informations sur l'enregistrement d'un nom de domaine

72. L'article 6 établit une procédure qui prévoit la coopération directe entre les autorités d'une Partie et une entité fournissant des services d'enregistrement de noms de domaine, située sur le territoire d'une autre Partie, pour obtenir des informations sur l'enregistrement de noms de domaine sur internet. Comme pour l'article 7, la procédure s'appuie sur les conclusions du Groupe

sur les preuves dans le nuage du Comité de la Convention sur la cybercriminalité, reconnaissant l'importance que revêt un accès transfrontalier rapide à des preuves électroniques pour des enquêtes ou des procédures pénales spécifiques, au vu des difficultés que posent les procédures existantes pour l'obtention de preuves électroniques.

73. La procédure reconnaît également le modèle actuel de gouvernance internet qui repose sur l'élaboration de politiques multiparties prenantes établies par consensus. Ces politiques sont normalement fondées sur le droit des contrats. La procédure visée dans cet article entend compléter ces politiques pour les objectifs de ce Protocole, autrement dit aux fins d'enquêtes ou de procédures pénales spécifiques. L'obtention des données d'enregistrement d'un nom de domaine constitue souvent une première étape indispensable pour de nombreuses enquêtes criminelles, et pour déterminer l'endroit où adresser des demandes de coopération internationale.

74. De nombreuses formes de cybercriminalité sont facilitées par le fait que des criminels créent et exploitent des domaines à des fins malveillantes et illicites. Ainsi, un nom de domaine peut être utilisé comme plateforme pour disséminer des maliciels, des botnets, mener des activités de phishing et autres activités de même genre, se livrer à la fraude ou encore à la diffusion de matériels de pédopornographie, ou à d'autres fins criminelles. L'accès aux informations sur la personne physique ou morale qui a enregistré le domaine (le « déclarant ») est donc critique pour identifier un suspect dans une enquête ou procédure pénale spécifique. Au départ, les données d'enregistrement des noms de domaine étaient accessibles à tous ; maintenant, certaines parties de l'information sont d'accès restreint, ce qui a des répercussions sur les missions de politique publique des services judiciaires et répressifs.

75. Les informations concernant l'enregistrement de noms de domaine sont détenues par des entités fournissant des services d'enregistrement de noms de domaine. Ces dernières prennent la forme d'organisations vendant des noms de domaine au public (les « registraires ») ainsi que d'opérateurs régionaux ou nationaux de registres qui conservent des bases de données officielles (les « registres ») de tous les noms de domaine enregistrés pour un domaine de premier niveau et qui acceptent des demandes d'enregistrement. Dans certains cas, ces informations peuvent constituer des données à caractère personnel et être protégées en vertu des dispositions de protection des données dans le droit interne de la Partie sur le territoire de laquelle se trouve l'entité concernée fournissant des services d'enregistrement de noms de domaine (registraire ou registre) ou la personne à laquelle se réfèrent les données.

76. L'objectif de l'article 6 est de donner un cadre effectif et efficient d'obtention d'informations pour identifier ou contacter la personne ayant enregistré un nom de domaine. Les modalités de sa mise en œuvre dépendent des considérations légales et politiques des différentes Parties. Cet article entend compléter les politiques et pratiques actuelles et futures de gouvernance de l'internet.

Paragraphe 1

77. En vertu du paragraphe 1, chaque Partie adopte les mesures nécessaires pour habilitier ses autorités compétentes à adresser des demandes directement à une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie, autrement dit sans demander aux autorités compétentes sur le territoire où l'entité est située d'intervenir en tant qu'intermédiaire. Le paragraphe 1 donne aux Parties une certaine flexibilité par rapport au format dans lequel les demandes sont présentées, car le format dépend des considérations juridiques et politiques respectives des Parties. Une Partie peut utiliser les procédures disponibles dans son système de droit interne, y compris l'émission d'une injonction ; toutefois, aux fins de l'article 6, une telle demande est traitée comme une demande non contraignante. La forme de la demande ou les effets qu'elle produit en vertu du droit interne de la Partie requérante n'affecterait donc pas le caractère volontaire de la coopération internationale au titre de l'article 6 et, si l'entité ne divulgue pas les informations recherchées, le paragraphe 5 de l'article 6 serait applicable.

78. Le libellé du paragraphe 1 est suffisamment générique pour reconnaître qu'une telle demande peut aussi être émise et les informations obtenues via une interface, un portail ou autre outil technique mis à disposition par des organisations. Ainsi, une organisation peut fournir une interface ou un outil de recherche pour faciliter ou accélérer la divulgation d'informations sur l'enregistrement d'un nom de domaine à la suite d'une demande. En revanche, plutôt que de viser un portail ou une interface spécifiques, l'article 6 utilise des termes neutres du point de vue technologique pour permettre une adaptation à l'évolution en la matière.

79. Comme cela est prévu à l'article 2, une demande en vertu du paragraphe 1 de l'article 6 peut être émise uniquement aux fins d'enquêtes ou procédures pénales spécifiques. L'expression « autorités compétentes » est définie à l'article 3, paragraphe 2.b, et désigne « une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par le présent protocole ». Une « entité fournissant des services d'enregistrement

de noms de domaine » renvoie actuellement aux registraires et registres. Pour prendre en compte la situation actuelle et dans le même temps permettre une adaptation pour le cas où les modèles économiques et l'architecture de l'internet changent au fil du temps, cet article utilise l'expression plus générique d'« entité fournissant des services d'enregistrement de noms de domaine ».

80. Si les informations pour identifier ou contacter la personne ayant enregistré un nom de domaine sont souvent stockées par des entités fournissant des services génériques d'enregistrement de noms de domaine dans le monde entier, ce qu'on appelle des « domaines génériques de premier niveau (generic top level domains ou gTLD), les Parties ont reconnu que des services plus spécifiques en matière d'enregistrement de noms de domaine liés à des entités nationales ou régionales (les domaines nationaux de premier niveau ou ccTLD) peuvent aussi être enregistrés par des personnes morales ou physiques dans d'autres pays, et peuvent également être utilisées par des criminels. L'article 6 ne se limite donc pas aux entités fournissant des gTLD, car les deux types de services concernant l'enregistrement de noms de domaine – ou les futurs types de services de ce genre – peuvent être utilisés pour perpétrer des actes de cybercriminalité.

81. La phrase « informations en vue d'identifier ou de contacter la personne ayant enregistré un nom de domaine » renvoie aux informations qui étaient auparavant publiquement accessibles par des outils de recherche connus sous l'acronyme WHOIS, par exemple le nom, l'adresse physique, l'adresse électronique et le numéro de téléphone d'une personne ayant enregistré un nom de domaine. Certaines Parties peuvent considérer ces informations comme un sous-ensemble des informations relatives aux abonnés au sens de l'article 18, paragraphe 3, de la Convention. Les informations d'enregistrement de noms de domaine sont des informations de base qui ne permettraient pas de tirer des conclusions précises concernant la vie privée et le modus vivendi de quelqu'un. Leur divulgation peut donc être moins intrusive que celle d'autres catégories de données.

Paragraphe 2

82. Le paragraphe 2 fait obligation à chaque Partie d'adopter des mesures pour permettre à des entités fournissant des services d'enregistrement de noms de domaine établies sur son territoire de divulguer ces informations en réponse à une demande visée au paragraphe 1, sous réserve des conditions raisonnables prévues par le droit interne, qui, dans certaines Parties, peuvent inclure des conditions découlant des lois sur la protection des données. En

même temps, l'article 14 limite la possibilité de refuser des transferts de données en vertu des règles de protection des données pour les transferts internationaux, et les facteurs du paragraphe 83 ont été inclus pour faciliter le traitement en vertu des règles de protection des données. Ces mesures devraient faciliter la divulgation des données demandées de manière rapide et efficace dans toute la mesure du possible.

83. L'article 6 ne fait pas obligation aux Parties d'adopter des textes législatifs contraignant ces entités à répondre à une demande émanant d'une autorité d'une autre Partie. Ainsi, l'entité offrant des services d'enregistrement de noms de domaine peut avoir besoin de déterminer si elle doit divulguer les informations recherchées. Le Protocole contribue à cette détermination en fournissant des garanties qui devraient faciliter la capacité des entités à répondre sans difficulté aux demandes au titre du présent article:

- le Protocole fournit ou oblige les Parties à fournir une base juridique pour les demandes ;
- l'article 6 exige que la demande provienne d'une autorité compétente (article 6, paragraphes 1 et 3.a, et paragraphe 79 et 84 de ce rapport explicatif) ;
- le Protocole prévoit qu'une demande est faite aux fins d'enquêtes ou de procédures pénales spécifiques (article 2) ;
- cet article exige que la demande contienne une déclaration selon laquelle le besoin de l'information découle de sa pertinence pour une enquête ou une procédure pénale spécifique et que l'information ne soit utilisée que pour cette enquête ou procédure pénale spécifique (article 6, paragraphe 3.c) ;
- le protocole prévoit des garanties pour le traitement des données à caractère personnel divulguées et transférées conformément à ces demandes au titre de l'article 14 ;
- les informations à divulguer sont limitées et ne permettraient pas de tirer des conclusions précises concernant la vie privée des personnes visées ;
- il est possible d'escompter des entités qu'elles coopèrent ou de les y obliger en vertu d'arrangements contractuels avec l'Internet Corporation for Assigned Names and Numbers (ICANN).

Paragraphe 3

84. Le paragraphe 3 de l'article 6 spécifie les informations qui, au minimum, doivent être fournies par une autorité formulant une demande en vertu du

paragraphe 1 de cet article. Ces informations sont particulièrement pertinentes pour l'exécution de la demande par l'entité fournissant des services d'enregistrement de noms de domaine. La demande devra inclure:

a. la date d'émission ainsi que l'identité et les coordonnées de l'autorité compétente qui émet la demande (paragraphe 3.a) (voir paragraphe 79 du présent rapport explicatif) ;

b. le nom de domaine au sujet duquel les informations sont demandées et une liste détaillée des informations recherchées, y compris les éléments de données spécifiques tels que le nom, l'adresse physique, l'adresse électronique ou le numéro de téléphone de la personne ayant enregistré un nom de domaine (paragraphe 3.b) ;

c. une déclaration selon laquelle la demande est émise conformément au présent Protocole ; par cette déclaration, la Partie atteste que la demande est conforme aux dispositions du Protocole (paragraphe 3.c). La Partie émettrice confirme également dans cette déclaration qu'elle a « besoin » de ces informations du fait de leur pertinence pour une enquête ou procédure pénale spécifique et que les informations ne seront utilisées que pour cette enquête ou procédure pénale spécifique. Si les Parties sont des pays européens, le critère du « besoin de ces informations » – autrement dit les informations qui doivent être nécessaires et proportionnées – pour une enquête ou procédure pénale devrait découler des principes de la Convention européenne des droits de l'homme et des libertés fondamentales du Conseil de l'Europe de 1950, de sa jurisprudence applicable et du droit et de la jurisprudence internes. Il découle de ces sources que la compétence ou la procédure devraient être proportionnelles à la nature et aux circonstances d'une infraction (voir paragraphe 146 du rapport explicatif de la Convention sur la cybercriminalité). D'autres Parties appliqueront les principes de leur droit interne adaptés tels que le principe de pertinence (en d'autres termes, la preuve recherchée par une demande doit être pertinente pour l'enquête ou les poursuites). Les parties devraient éviter les demandes générales de divulgation d'informations concernant les noms de domaine, à moins qu'elles ne soient nécessaires pour l'enquête ou la procédure pénale spécifique ;

d. l'échéance et les modalités de divulgation des informations et autres instructions procédurales spéciales (paragraphe 3.d) ; l'expression « instructions procédurales spéciales » entend inclure toute demande de confidentialité, notamment une demande de non-divulgation de la demande à la personne ayant enregistré un nom de domaine ou à un autre tiers. Si la confidentialité

est demandée pour éviter une divulgation prématurée de l'affaire, cela devrait figurer dans la demande. Dans certaines Parties, la confidentialité de la demande sera appliquée automatiquement par dispositions légales, alors que dans d'autres ce ne sera pas nécessairement le cas. C'est pourquoi, là où la confidentialité est nécessaire, les Parties sont encouragées à examiner les informations publiquement accessibles et à demander des conseils aux autres Parties concernant le droit applicable ainsi que des politiques des entités fournissant des services d'enregistrement de noms de domaine concernant l'information d'un abonné/personne ayant enregistré un nom de domaine avant de soumettre à l'entité une demande en vertu du paragraphe 1 de l'article 6. En outre, les instructions procédurales spéciales peuvent prévoir la spécification du canal de transmission le plus adapté aux besoins de l'autorité.

85. Le paragraphe 3 ne prévoit pas d'obligation d'inclure un descriptif des faits dans la demande, étant donné que ces informations sont confidentielles dans la plupart des enquêtes criminelles et ne peuvent être divulguées à une partie privée. Toutefois, l'entité qui reçoit une demande au titre du présent article peut avoir besoin de certaines informations supplémentaires qui lui permettraient de prendre une décision positive concernant la demande. Par conséquent, l'entité peut demander un complément d'informations lorsque, sans celles-ci, elle n'est pas en mesure d'exécuter la demande.

Paragraphe 4

86. L'objectif du paragraphe 4 est d'encourager l'utilisation de moyens électroniques lorsque ceux-ci sont acceptables pour l'entité fournissant des services d'enregistrement de noms de domaine, car ce sont presque toujours les moyens de communication les plus efficaces et les plus rapides. En conséquence, si cela est acceptable pour l'entité fournissant des services d'enregistrement de noms de domaine, une Partie peut soumettre une demande à l'entité sous forme électronique, par exemple en utilisant le courrier électronique, les portails électroniques ou d'autres moyens. Bien que l'on suppose que les entités préfèrent recevoir les demandes sous cette forme, il ne s'agit pas d'une exigence. Comme le prévoient d'autres articles du présent Protocole autorisant les ordonnances ou les demandes sous forme électronique (tels que les articles 7, 8 et autres), des niveaux appropriés de sécurité et d'authentification peuvent être exigés. Les parties et les entités peuvent décider elles-mêmes si des voies ou des moyens de transmission et d'authentification sécurisés sont disponibles, ou si des protections de sécurité spéciales (y compris le cryptage) peuvent être nécessaires dans un cas sensible particulier.

Paragraphe 5

87. Bien que cette disposition relève des « demandes » et non des « injonctions » contraignantes pour la divulgation de données d'enregistrement de noms de domaine, il est escompté que l'entité destinataire de la demande sera en mesure de divulguer les informations demandées en vertu de cette disposition, une fois les conditions applicables satisfaites. Si l'entité ne divulgue pas les informations demandées, d'autres mécanismes pourraient être envisagés pour les obtenir, en fonction des circonstances. Le paragraphe 5 prévoit donc une consultation entre les Parties concernées pour obtenir des informations supplémentaires et déterminer quels mécanismes peuvent, par exemple, être activés pour améliorer une coopération future. Afin de faciliter les consultations, le paragraphe 5 dispose également qu'une Partie requérante peut demander des informations complémentaires à une entité. Les entités sont encouragées à motiver leur refus de divulguer les données demandées en réponse à une telle demande.

Paragraphe 6

88. Le paragraphe 6 impose que les Parties désignent, au moment de la signature de ce Protocole ou du dépôt de leur instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, une autorité aux fins de la consultation prévue au paragraphe 5. La désignation d'un point de contact dans l'État partie où est située l'entité aidera la Partie requérante à déterminer rapidement les mesures auxquelles il est possible de recourir pour obtenir les données souhaitées dans le cas où l'entité refuse d'accéder à une requête directe adressée en vertu de l'article 6.

Paragraphe 7

89. Le paragraphe 7 est explicite et dispose que le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées en vertu du paragraphe 6 et que chaque Partie veille à ce que les données qu'elle a fournies pour le registre soient correctes à tout moment.

Article 7 – Divulgence des informations sur les abonnés

90. L'article 7 établit une procédure prévoyant la coopération directe entre les autorités d'une Partie et un fournisseur de services sur le territoire d'une autre Partie en vue d'obtenir des données relatives aux abonnés. Cette procédure repose sur les conclusions du Groupe de travail du Comité de la Convention sur les preuves dans le nuage et sur la Note d'orientation du Comité relative à l'article 18 de la Convention, reconnaissant l'importance de

l'accès transfrontalier en temps opportun aux éléments de preuve électroniques dans les enquêtes ou les procédures pénales spécifiques, eu égard aux difficultés que posent les procédures existantes pour obtenir des éléments de preuve électroniques auprès des fournisseurs de services dans d'autres pays.

91. Un nombre croissant d'enquêtes ou de procédures pénales nécessitent aujourd'hui d'avoir accès à des éléments de preuve électroniques détenus par des fournisseurs de services dans d'autres pays. Même dans le cas d'infractions strictement internes par nature – c'est-à-dire lorsque le crime, la victime et l'auteur se trouvent tous dans le pays où a lieu l'infraction, de même que l'autorité chargée de l'enquête – les éléments de preuve électroniques peuvent être détenus par un fournisseur de services sur le territoire d'un autre pays. Dans bien des situations, les autorités qui enquêtent sur une infraction peuvent être amenées à recourir à des procédures de coopération internationale, comme l'entraide judiciaire, qui ne permettent pas toujours d'obtenir une aide rapide ou suffisamment efficace pour répondre aux besoins de l'enquête ou de la procédure en raison du volume des demandes de preuves électroniques, qui ne cesse d'augmenter.

92. Les données relatives aux abonnés sont les informations les plus fréquemment recherchées dans les enquêtes pénales relatives à la cybercriminalité et à d'autres types d'infractions qui nécessitent l'obtention de preuves électroniques. Elles indiquent l'identité d'un abonné à un service particulier, son adresse et des informations similaires visées à l'article 18, paragraphe 3, de la Convention. Ces données ne permettent pas de tirer des conclusions précises sur la vie privée et les habitudes quotidiennes des personnes concernées, ce qui signifie que leur divulgation peut être moins intrusive que celle d'autres catégories de données.

93. Les données relatives aux abonnés sont définies à l'article 18, paragraphe 3, de la Convention (incorporées à l'article 3, paragraphe 1, de ce Protocole) selon lequel « toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ; c. toute autre information relative à l'endroit où

se trouvent les équipements de communication, disponible sur la base du contrat ou de l'arrangement de service » (voir aussi le rapport explicatif de la Convention, paragraphes 177 à 183). Les informations nécessaires à l'identification d'un abonné à un service peuvent inclure certaines données relatives à l'adresse IP – l'adresse IP utilisée au moment de la création du compte, l'adresse IP utilisée le plus récemment pour se connecter au service ou les adresses IP utilisées pour se connecter à un moment précis, par exemple. Dans certains États parties, ces informations sont traitées comme des données relatives au trafic pour diverses raisons, notamment parce qu'elles sont considérées comme ayant trait à la transmission d'une communication. En conséquence, le paragraphe 9.b de l'article 7 prévoit une possibilité de réserve pour certaines Parties.

94. Bien que l'article 18 de la Convention traite déjà de certains aspects de la nécessité d'un accès rapide et effectif aux preuves électroniques détenues par des fournisseurs de services, il n'apporte pas à lui seul une solution complète à ce problème, étant donné qu'il s'applique dans des circonstances plus limitées. Plus précisément, l'article 18 de la Convention s'applique lorsqu'un fournisseur de services se trouve « sur le territoire » de la Partie émettrice (voir article 18, paragraphe 1.a, de la Convention) ou « offre ses prestations » dans la Partie émettrice (voir article 18, paragraphe 1.b, de la Convention). Compte tenu des limites de l'article 18 et des difficultés qui se posent dans la mise en œuvre de l'entraide judiciaire, il a été jugé important d'établir un mécanisme complémentaire qui permettrait un accès transfrontalier plus effectif aux informations nécessaires aux enquêtes ou aux procédures pénales spécifiques. En conséquence, le champ d'application de l'article 7 du Protocole est plus étendu que celui de l'article 18 de la Convention, car il permet à une Partie d'adresser certaines injonctions aux fournisseurs de services sur le territoire d'une autre Partie. Les Parties ont reconnu que, bien que de telles injonctions adressées directement par les autorités d'une Partie à des fournisseurs de services situés dans une autre Partie soient souhaitables pour favoriser un accès rapide et efficace aux données requises, il ne devrait pas être permis à une Partie d'employer tous les mécanismes d'exécution prévus par son droit interne pour faire exécuter ces injonctions. Pour cette raison, l'exécution de ces injonctions, dans les cas où le fournisseur ne divulgue pas les données relatives aux abonnés demandées, est limitée à la manière énoncée au paragraphe 7 de l'article 7. Cette procédure prévoit des garanties permettant de tenir compte des exigences particulières découlant d'une coopération directe entre les autorités d'une Partie et les fournisseurs de services se trouvant sur le territoire d'une autre Partie.

95. Comme cela est indiqué à l'article 5, paragraphe 7, le présent article est sans préjudice de la capacité des Parties à exécuter les injonctions adressées en application de l'article 18 de la Convention ou de toute autre manière autorisée par celle-ci, et ne porte pas non plus atteinte à la coopération (y compris une coopération spontanée) entre Parties, ou entre Parties et fournisseurs de services, au moyen d'autres accords, dispositions, pratiques ou lois nationales.

Paragraphe 1

96. Le paragraphe 1 impose aux Parties de conférer aux autorités compétentes les pouvoirs nécessaires pour adresser à un fournisseur de services sur le territoire d'une autre Partie une injonction de produire des données relatives aux abonnés. Cette injonction ne peut être émise qu'aux fins d'obtention de données spécifiées et stockées relatives à des abonnés.

97. Le paragraphe 1 prévoit également l'obligation selon laquelle les injonctions ne peuvent être émises et adressées que dans le cadre d'« enquêtes ou de procédures pénales spécifiques » menées par le pays émetteur, au sens de l'article 2 du Protocole. En outre, les injonctions ne peuvent être émises que pour obtenir des informations « nécessaires » à l'enquête ou à la procédure en question. Pour les pays européens, les informations requises – qui doivent être nécessaires et proportionnées – pour une enquête ou une procédure pénale doivent respecter les principes issus de la Convention européenne des droits de l'homme et des libertés fondamentales, de sa jurisprudence applicable, ainsi que de la législation et de la jurisprudence nationales. D'après ces principes, les pouvoirs ou les procédures doivent être proportionnelles à la nature et aux circonstances de l'infraction (voir paragraphe 146 du rapport explicatif de la Convention sur la cybercriminalité). D'autres Parties mettront en œuvre des principes connexes de leur droit interne, comme les principes de pertinence (l'élément de preuve demandé au moyen de l'injonction doit être pertinent pour l'enquête ou les poursuites engagées) et de limitation de la portée des injonctions de produire des données relatives aux abonnés, pour éviter qu'elle soit trop large. Cette restriction souligne le principe déjà énoncé à l'article 2 du Protocole et au paragraphe 1 de l'article 7, qui limite la mesure à des enquêtes et procédures pénales spécifiques, selon lequel ces dispositions ne peuvent être utilisées pour obtenir la communication de données en masse (voir également le rapport explicatif, paragraphe 182, de la Convention).

98. Comme cela est défini au paragraphe 2.b de l'article 3, l'expression « autorités compétentes » désigne une autorité judiciaire, administrative ou autre

autorité chargée de l'application de la loi qui est habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution des mesures prévues par le présent Protocole. La même approche est prévue aux fins de la procédure de coopération directe visée dans cet article. En conséquence, l'ordre juridique national d'une Partie détermine quelle autorité est considérée comme une autorité compétente pour adresser une injonction. Bien que la Partie émettrice définisse laquelle de ses autorités est habilitée à émettre l'injonction, l'article 7 prévoit une garantie, à son paragraphe 5, selon lequel la Partie destinataire peut exiger qu'une autorité désignée examine les injonctions adressées en application de cet article et ait la possibilité de mettre fin à la coopération directe, comme cela est décrit plus loin.

99. À l'article 7, l'expression « fournisseur de services sur le territoire d'une autre Partie » nécessite que le fournisseur de services soit physiquement présent sur le territoire de l'autre Partie. En vertu de cet article, le simple fait, par exemple, qu'un fournisseur de services ait établi une relation contractuelle avec une entreprise dans un État partie, mais que le fournisseur de services lui-même ne soit pas physiquement présent sur le territoire de cette Partie, ne permettrait pas de considérer que le fournisseur de services se trouve « sur le territoire » de cette Partie. Le paragraphe 1 exige, en outre, que les données soient en la possession ou sous le contrôle du fournisseur de services.

Paragraphe 2

100. Aux termes du paragraphe 2 de l'article 7, les Parties sont tenues d'adopter toutes les mesures nécessaires pour que les fournisseurs de services sur leur territoire répondent à une injonction adressée par une autorité compétente dans une autre Partie, conformément au paragraphe 1. Compte tenu des différences entre les systèmes juridiques nationaux, les Parties peuvent mettre en œuvre des mesures différentes pour appliquer une procédure permettant d'établir une coopération directe de manière efficace et efficiente. Ces dispositions peuvent aller de l'élimination des obstacles juridiques auxquels se heurtent les fournisseurs de services pour répondre à une injonction à la mise en place d'une base positive obligeant les fournisseurs de services à répondre à une injonction adressée par une autorité d'un autre État partie de manière efficace et efficiente. Chaque Partie doit veiller à ce que les fournisseurs de services puissent se conformer en toute légalité aux injonctions visées par l'article 7 d'une manière qui garantisse la sécurité juridique, de sorte que les fournisseurs de services ne voient pas leur responsabilité juridique engagée du seul fait qu'ils se sont conformés de bonne foi à une injonction adressée en vertu du paragraphe 1 et pour laquelle une Partie a déclaré qu'elle était émise

en application du présent Protocole (article 7, paragraphe 3.b). Cela n'exclut pas que cette responsabilité soit engagée pour d'autres raisons que le fait d'avoir suivi l'injonction, comme un manquement à une quelconque obligation légale applicable selon laquelle un fournisseur de services doit assurer des conditions de sécurité suffisantes pour les données stockées. La forme de la mise en œuvre dépend des considérations juridiques et politiques des Parties ; pour les Parties qui ont des exigences en matière de protection des données, il s'agirait notamment de définir une base claire pour le traitement des données à caractère personnel. Au vu des exigences supplémentaires prévues par les lois sur la protection des données pour autoriser d'éventuels transferts internationaux de données relatives aux abonnés, le présent Protocole traduit l'importance de l'intérêt public pour cette mesure de coopération directe et prévoit à son article 14 les garanties requises à cette fin.

101. Comme cela est énoncé ci-dessus, l'ordre juridique national d'une Partie détermine quelle autorité est considérée comme une autorité compétente pour adresser une injonction. Certaines Parties ont estimé nécessaire de disposer d'une garantie supplémentaire permettant un contrôle plus poussé de la légalité de l'injonction (voir par exemple le paragraphe 98 ci-dessus) en raison du caractère direct de la coopération. Alors que la Partie émettrice définit parmi ses autorités celles chargées d'adresser l'injonction, le paragraphe 2.b autorise les Parties à faire une déclaration selon laquelle « l'injonction adressée en application de l'article 7, paragraphe 1, doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante ». Une Partie faisant usage de cette possibilité doit accepter toute injonction émise par l'une des autorités citées ou sous la supervision de l'une d'elles.

Paragraphe 3

102. Le paragraphe 3 de l'article 7 précise les informations qui doivent, au minimum, être fournies par une autorité adressant une injonction en application du paragraphe 1 de cet article, bien qu'une Partie émettrice puisse décider d'inclure des renseignements complémentaires dans l'injonction elle-même pour faciliter son traitement ou parce que son droit interne lui impose de les y faire figurer. Les informations visées au paragraphe 3 sont particulièrement pertinentes pour l'exécution de l'injonction par le fournisseur de services, ainsi que pour l'intervention éventuelle de l'autorité de l'État partie dans lequel se trouve le fournisseur de services, conformément au paragraphe 5. L'injonction doit mentionner le nom de l'autorité émettrice et la date d'émission, donner des informations permettant d'identifier le fournisseur de services, préciser

l'infraction qui fait l'objet de l'enquête ou de la procédure pénale, désigner l'autorité qui sollicite les données relatives aux abonnés et présenter une description détaillée des données spécifiques relatives aux abonnés qui sont demandées. L'injonction doit également contenir une déclaration selon laquelle elle est émise en application du présent Protocole ; en faisant cette déclaration, la Partie indique que l'injonction est conforme aux dispositions du Protocole.

103. En ce qui concerne la différence entre le paragraphe 3.a (l'autorité émettrice) et le paragraphe 3.d (l'autorité qui sollicite les données relatives aux abonnés), dans certaines Parties, l'autorité émettrice et l'autorité qui sollicite les données sont distinctes. Ainsi, les enquêteurs ou les procureurs peuvent jouer le rôle de l'autorité qui sollicite les données, alors que l'injonction est adressée par un juge. Dans de telles situations, il est alors nécessaire d'identifier l'autorité qui sollicite les données et celle qui émet l'injonction.

104. Il n'est pas nécessaire de produire un exposé des faits, étant donné que ces informations sont confidentielles dans la plupart des enquêtes pénales et qu'elles ne peuvent être divulguées à une partie privée.

Paragraphe 4

105. Alors que le paragraphe 3 énonce les informations qui doivent, au minimum, être transmises lors de l'émission d'une injonction au titre du paragraphe 1, ces injonctions ne peuvent souvent être exécutées que si le fournisseur de services (et, le cas échéant, l'autorité désignée par la Partie destinataire en application du paragraphe 5) reçoit des informations complémentaires. Par conséquent, le paragraphe 4 de l'article 7 précise qu'une autorité émettrice doit fournir des informations complémentaires sur le fondement juridique interne qui habilite l'autorité à adresser une injonction ; mentionner les dispositions juridiques et les sanctions applicables à l'infraction qui est à l'origine d'une enquête ou de poursuites ; donner les coordonnées de l'autorité à laquelle le fournisseur de services doit communiquer les données relatives aux abonnés, demander de plus amples informations ou adresser toute autre réponse ; indiquer le délai et le mode de communication de ces données ; spécifier si une demande de conservation des données a été formulée précédemment, en précisant la date de conservation et tout numéro de référence applicable ; évoquer tout type d'instructions spéciales en matière de procédure (demandes de confidentialité ou d'authentification) ; déclarer, le cas échéant, que la notification simultanée a été faite conformément au paragraphe 5 ; et ajouter toute autre information qui pourrait aider à obtenir la divulgation des données relatives aux abonnés. Il n'est pas nécessaire que

les coordonnées fournies concernent précisément une personne, mais qu'elles concernent seulement une entité administrative. Ces renseignements complémentaires peuvent être transmis séparément mais peuvent également être inclus dans l'injonction elle-même, si la législation de la Partie émettrice le permet. L'injonction comme les informations complémentaires sont transmises directement au fournisseur de services.

106. Les instructions spéciales en matière de procédure portent notamment sur toute demande de confidentialité, y compris les demandes de non-divulgence de l'injonction à l'abonné concerné ou à d'autres tiers, sauf que les instructions spéciales de procédure ne peuvent empêcher le fournisseur de consulter les autorités à notifier en vertu du paragraphe 5.a ou à consulter en vertu du paragraphe 5.b. Si des mesures de confidentialité sont nécessaires pour éviter une divulgation prématurée de l'affaire, il faut l'indiquer dans la demande. Dans certains États parties, la confidentialité de l'injonction est maintenue de plein droit, alors que dans d'autres États parties ce n'est pas nécessairement le cas. Par conséquent, afin d'éviter tout risque de divulgation prématurée de l'enquête, les Parties sont encouragées à prendre connaissance de la législation applicable et des politiques des fournisseurs de services en matière de notification des abonnés, avant d'adresser l'injonction au fournisseur de services en application du paragraphe 1. En outre, au titre des instructions spéciales en matière de procédure, le moyen de transmission le plus adapté aux besoins de l'autorité peut être spécifié. Le fournisseur de services peut également demander des renseignements complémentaires concernant le compte ou d'autres informations pour l'aider à fournir une réponse rapide et complète. Une demande de confidentialité ne devrait pas empêcher les fournisseurs de services de rendre compte, dans un souci de transparence, des nombres agrégés anonymes d'ordres reçus au titre de l'article 7.

Paragraphe 5

107. Aux termes du paragraphe 5.a, une Partie peut notifier au Secrétaire Général du Conseil de l'Europe que, lorsqu'une injonction est émise en vertu du paragraphe 1 à l'intention d'un fournisseur de services sur son territoire, elle exigera une notification simultanée soit dans tous les cas (c'est-à-dire pour toutes les injonctions transmises aux fournisseurs de services sur son territoire), soit dans des circonstances déterminées.

108. En application du paragraphe 5.b, une Partie peut également, en vertu de son droit interne, exiger d'un fournisseur de services qui se voit adresser une injonction par une autre Partie qu'il la consulte dans certaines circonstances

déterminées. Une Partie ne peut pas exiger d'être consultée pour chaque injonction, car cela ajouterait une mesure supplémentaire qui pourrait entraîner un retard considérable, mais seulement dans des circonstances limitées et définies. L'obligation de procéder à une consultation devrait être limitée aux circonstances dans lesquelles il y a un risque accru de devoir imposer des conditions ou invoquer un motif de refus ou une crainte de préjudice potentiel pour les enquêtes ou procédures pénales menées par la Partie transférante.

109. Les procédures de notification et de consultation sont laissées à l'entière discrétion des Parties, qui ne sont pas tenues d'exiger l'une ou l'autre.

110. Les Parties notifiées en vertu du paragraphe 5.a ou consultées en vertu du paragraphe 5.b peuvent ordonner à un fournisseur de services de ne pas divulguer des informations pour les motifs prévus au paragraphe 5.c, qui sont décrits plus en détail au paragraphe 141 du présent rapport explicatif sur l'article 8. De ce fait, la capacité d'une partie à être avisée ou consultée constitue une garantie supplémentaire. Cela dit, la coopération doit en principe être étendue et les obstacles à celle-ci strictement limités. En conséquence, comme l'expliquent les paragraphes 242 et 253 du rapport explicatif de la Convention, la détermination par la Partie avisée ou consultée des conditions et des refus qui s'appliqueraient en vertu des articles 25, paragraphe 4, et 27, paragraphe 4, de la Convention devrait également être limitée conformément aux objectifs de l'article 7 du présent Protocole, à savoir éliminer les obstacles à l'accès transfrontalier aux preuves électroniques aux fins d'enquêtes pénales et prévoir des procédures plus efficaces et accélérées dans ce domaine.

111. En vertu de paragraphe 5.d, les Parties qui font une déclaration en application du paragraphe 5.a ou qui exigent une consultation au titre du paragraphe 5.b peuvent contacter l'autorité désignée en vertu de l'article 4.c et lui demander des renseignements complémentaires pour déterminer s'il y a lieu, en vertu du paragraphe 5.c, d'ordonner au fournisseur de services de ne pas se conformer à l'injonction. Le processus se veut aussi rapide que les circonstances le permettent. La Partie notifiée ou consultée doit recueillir les informations nécessaires et prendre leur décision en vertu du paragraphe 5.c « dans les plus brefs délais ». Le cas échéant, pour permettre la coopération, la procédure visée au paragraphe 5.d peut également fournir l'occasion de clarifier certains aspects de la confidentialité des informations recherchées ainsi que toute limitation d'utilisation envisagée par l'autorité sollicitant les données. Cette Partie doit également informer rapidement les autorités de la Partie émettrice si elle décide d'ordonner au fournisseur de services de ne pas répondre favorablement, en indiquant les raisons de cette décision.

112. Une Partie qui exige d'être informée ou consultée peut décider d'imposer au fournisseur un délai d'attente avant qu'il ne fournisse les données relatives aux abonnés en réponse à l'injonction, afin de permettre la communication d'informations ou la tenue de la consultation et toute formulation de demandes de renseignements complémentaires par la Partie.

113. Aux termes du paragraphe 5.e, une Partie qui exige d'être informée ou consultée doit désigner une autorité unique et, lorsqu'une notification est requise en vertu du paragraphe 5.a, communiquer au Secrétaire Général du Conseil de l'Europe les coordonnées de cette autorité.

114. Une Partie peut modifier son exigence de notification ou de consultation à tout moment, selon les facteurs qu'elle juge pertinents, par exemple si elle souhaite passer d'un système de notification à un système de consultation ou si elle est suffisamment à l'aise avec la coopération directe pour pouvoir revoir ou annuler une obligation de notification ou de consultation adoptée précédemment. Elle peut également décider que, compte tenu de l'expérience qu'elle a acquise dans l'utilisation du mécanisme de coopération directe, elle souhaite instaurer un système de notification ou de consultation.

115. En vertu du paragraphe 5.f, le Secrétaire Général du Conseil de l'Europe est tenu d'établir et de tenir à jour un registre de toutes les exigences des Parties en matière de notification en vertu des paragraphes 5.a et 5.e. La mise à disposition d'un registre public et à jour est essentielle pour garantir que les autorités de la Partie émettrice et les fournisseurs de services sont informés des exigences de notification de chaque Partie, lesquelles, comme indiqué ci-dessus, peuvent être modifiées à tout moment. Étant donné que toutes les Parties peuvent apporter une telle modification à leur discrétion, chaque Partie qui apporte une modification ou relève une inexactitude concernant ses données dans le registre est tenue d'en aviser immédiatement le Secrétaire Général afin de s'assurer que les autres Parties ont connaissance des exigences en vigueur et peuvent les appliquer correctement.

Paragraphe 6

116. Le paragraphe 6 indique clairement que la communication d'informations à une autre Partie et la fourniture d'informations supplémentaires par voie électronique, y compris par l'utilisation de courrier électronique et de portails électroniques, sont autorisées. Si le fournisseur de services le juge acceptable, une Partie peut soumettre une injonction en vertu du paragraphe 1 et des informations supplémentaires en vertu du paragraphe 4 sous forme électronique. L'objectif est d'encourager le recours à des moyens

électroniques s'ils sont acceptables pour le fournisseur de services, car ce sont presque toujours les moyens de communication les plus efficaces et les plus rapides. Les méthodes d'authentification appliquées peuvent comprendre divers moyens, utilisés éventuellement en les associant, pour permettre une identification sécurisée de l'autorité requérante. Ces moyens peuvent par exemple être les suivants: l'obtention d'une confirmation d'authenticité par l'intermédiaire d'une autorité connue au sein de la Partie émettrice (auprès de l'expéditeur ou d'une autorité centrale ou désignée, par exemple) ; des communications ultérieures entre l'autorité émettrice et la Partie destinataire ; l'utilisation d'une adresse électronique officielle ou de futures méthodes de vérification technologique qui peuvent être facilement utilisées par les autorités qui transmettent les informations. Des dispositions similaires figurent au paragraphe 2 de l'article 10 et d'autres orientations concernant les exigences en matière de sécurité sont proposées au paragraphe 174 du présent rapport explicatif. L'article 6, paragraphe 4, et l'article 8, paragraphe 5, du présent Protocole contiennent également des dispositions similaires.

Paragraphe 7

117. Le paragraphe 7 prévoit que, si un fournisseur de services ne se conforme pas à l'injonction adressée au titre de l'article 7, la Partie émettrice ne peut en demander l'exécution qu'en application de l'article 8 ou d'une autre forme d'entraide. Les Parties qui invoquent cet article ne peuvent chercher à obtenir une exécution unilatérale.

118. S'agissant de l'exécution de l'injonction au moyen de l'article 8, le Protocole envisage une procédure simplifiée de conversion d'une injonction émise en vertu de cet article en une injonction émise en application de l'article 8 afin qu'il soit plus facile, pour la Partie émettrice, d'obtenir des données relatives aux abonnés.

119. Afin d'éviter les doubles emplois, une Partie émettrice doit accorder au fournisseur de services un délai de 30 jours ou le délai prévu au paragraphe 4.d, la plus longue période étant retenue, pour que le processus de notification et de consultation ait lieu et que le fournisseur de services communique les informations demandées ou indique son refus de le faire. Ce n'est qu'après l'expiration de ce délai, ou si le fournisseur a indiqué son refus de se conformer à l'injonction avant l'expiration de ce délai, qu'une Partie émettrice peut demander son exécution au titre de l'article 8 ou d'autres formes d'entraide. Pour permettre aux autorités d'évaluer s'il y a lieu de demander l'exécution en

vertu du paragraphe 7, les fournisseurs de services sont encouragés à donner les raisons pour lesquelles ils n'ont pas transmis les données demandées. Un fournisseur de services peut par exemple expliquer que ces données ne sont plus disponibles.

120. Si une autorité informée en application du paragraphe 5.a ou consultée au titre du paragraphe 5.b a informé la Partie émettrice que le fournisseur de services a reçu instruction de ne pas divulguer les informations demandées, la Partie émettrice peut néanmoins demander l'exécution de son injonction au moyen de l'article 8 ou d'une autre forme d'entraide. Toutefois, il existe un risque de rejet de cette nouvelle demande. Il est conseillé à la Partie émettrice de consulter à l'avance une autorité désignée en application des paragraphes 5.a ou 5.b afin de remédier à toute insuffisance de l'injonction initiale et d'éviter de transmettre des injonctions au moyen de l'article 8 ou de tout autre mécanisme d'entraide qui pourrait donner lieu à un refus.

Paragraphe 8

121. Aux termes du paragraphe 8, une Partie peut déclarer qu'une autre Partie doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en application de l'article 8, à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait. Ainsi, une Partie peut faire une telle déclaration parce qu'elle considère que les procédures prévues par cet article devraient permettre aux autres Parties d'obtenir des données relatives aux abonnés plus rapidement qu'en invoquant l'article 8 et, par conséquent, pourraient réduire le nombre de cas dans lesquels l'article 8 doit être invoqué. Les procédures prévues à l'article 8 ne seraient alors utilisées que lorsque les démarches visant à obtenir la divulgation de données relatives aux abonnés directement auprès du fournisseur de services ont échoué, lorsque la Partie émettrice a une explication raisonnable pour ne pas appliquer cet article en premier lieu ou lorsque la Partie émettrice s'est réservé le droit de ne pas appliquer cet article. Une Partie émettrice peut ainsi en faire la démonstration lorsqu'un fournisseur de services s'abstient régulièrement de transmettre des données relatives aux abonnés en réponse à des injonctions adressées directement par cette Partie. Autre exemple, si une Partie émettrice, au moyen d'une injonction unique, demande la divulgation de données relatives aux abonnés et de données relatives au trafic à une autre Partie qui applique l'article 8 à ces deux catégories de données, la Partie émettrice n'a pas besoin de demander dans un premier temps les données relatives aux abonnés séparément.

Paragraphe 9

122. En vertu du paragraphe 9.a, une Partie qui se réserve le droit de ne pas appliquer cet article n'est pas tenue de prendre des mesures en application du paragraphe 2 pour que les fournisseurs de services sur son territoire divulguent des données relatives aux abonnés en réponse à des injonctions adressées par d'autres Parties. Une Partie qui se réserve ce droit n'est pas autorisée à adresser des injonctions au titre du paragraphe 1 à des fournisseurs de services sur le territoire d'autres Parties.

123. Le paragraphe 9.b dispose que – pour les raisons mentionnées au paragraphe 93 ci-dessus – si la divulgation de certains types de numéros d'accès en vertu de cet article est incompatible avec les principes fondamentaux de son ordre juridique interne, une Partie peut se réserver le droit de ne pas appliquer cet article à ces numéros. Une Partie qui formule une telle réserve n'est pas autorisée à adresser des injonctions concernant ces numéros au titre du paragraphe 1 à des fournisseurs de services sur le territoire d'autres Parties.

Section 3 – Procédures complétant la coopération internationale entre autorités pour la divulgation de données informatiques stockées

Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic

124. L'article 8 a pour but de donner à une Partie requérante la capacité d'émettre une injonction à produire à une autre Partie requise, dans le cadre d'une demande, et de faire en sorte que la Partie requise soit en mesure de donner effet à ladite injonction en ordonnant à un fournisseur de services sur son territoire de produire des informations sur l'abonné ou des données relatives au trafic qui sont en possession ou sous le contrôle du fournisseur de services.

125. Cet article établit un mécanisme qui complète les dispositions de la Convention relatives à l'entraide judiciaire. Il est conçu pour être plus simple que l'entraide judiciaire actuelle, puisque les informations que doit fournir la Partie requérante sont plus limitées et le processus d'obtention des données plus rapide. Il complète sans pour autant remplacer d'autres processus d'entraide judiciaire prévus par la Convention, ou d'autres accords multilatéraux ou bilatéraux, qu'une Partie demeure libre d'invoquer. De fait, lorsqu'une Partie

requérante souhaite demander des données relatives au trafic à une Partie qui a émis une réserve concernant cet aspect de l'article 8, la Partie requérante peut recourir à une autre procédure d'entraide judiciaire. Lorsque, comme c'est fréquemment le cas, la demande porte sur la production simultanée d'informations sur l'abonné, de données relatives au trafic et de données relatives au contenu stocké, il peut être plus efficient de demander les trois formes de données à partir du même compte au moyen d'une seule demande d'entraide traditionnelle plutôt que de demander certains types de données au moyen de la méthode prévue par cet article pour d'autres types de données au moyen d'une demande d'entraide distincte.

Paragraphe 1

126. Le paragraphe 1 dispose que la Partie requérante doit être en mesure d'émettre une injonction en vue d'obtenir des informations relatives à l'abonné ou données relatives au trafic détenues par un fournisseur de services sur le territoire d'une autre Partie. Le terme « injonction » utilisé à l'article 8 signifie tout processus judiciaire ayant pour but d'obliger un fournisseur de services à fournir des informations relatives à un abonné ou données relatives au trafic. L'injonction peut ainsi prendre la forme d'une injonction de produire, d'une assignation ou autre mécanisme autorisé en droit et qui peut être émis pour ordonner la production d'informations relatives à un abonné ou données relatives au trafic.

127. Tel que cela est défini au paragraphe 2.b de l'article 3, l'expression « autorité compétente » au paragraphe 1 de l'article 8 recouvre « une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures visées par le présent Protocole aux fins du recueil ou de la production de preuves concernant des enquêtes ou procédures pénales spécifiques ». On relèvera que les autorités compétentes pour émettre une injonction en vertu du paragraphe 1 ne seront pas nécessairement les mêmes que les autorités désignées pour soumettre l'injonction à laquelle il convient de donner effet conformément au paragraphe 10.a de l'article 8, comme cela est décrit ci-dessous de manière plus détaillée.

128. À l'article 8, un fournisseur de services sur le territoire d'une autre Partie requiert que le fournisseur de services soit physiquement présent sur le territoire de l'autre Partie. En vertu de cet article, le simple fait que, par exemple, un fournisseur de services ait établi une relation contractuelle avec une société dans une Partie, mais qu'il ne soit pas lui-même physiquement présent dans

cette Partie ne le qualifierait comme étant « sur le territoire » de cette Partie. Le paragraphe 1 requiert en outre que les données soient en possession ou sous le contrôle du fournisseur de services.

Paragraphe 2

129. En vertu du paragraphe 2, la Partie requise adopte les mesures nécessaires aux fins de donner effet sur son territoire à une injonction émise en vertu du paragraphe 1, sous réserve des garanties qui vont être décrites ci-après. « Donner effet » signifie que la Partie requise devra ordonner au fournisseur de services de communiquer les informations relatives à l'abonné et les données relatives au trafic en utilisant le mécanisme correspondant au choix de la Partie requise, à condition que le mécanisme rende l'injonction exécutoire dans le droit interne de la Partie requise et respecte les dispositions du présent article. Par exemple, une Partie requise peut donner effet à l'injonction émanant d'une Partie requérante en acceptant l'injonction comme étant équivalente à des injonctions émises dans son droit interne, en l'endossant pour lui donner la même force exécutoire qu'une injonction émise dans son droit interne ou en émettant sa propre injonction de production. Quel que soit le mécanisme choisi, il sera soumis aux dispositions du droit interne de la Partie requise, puisque ce sont les procédures de cette dernière qui l'encadreront. La Partie requise peut ainsi s'assurer que son propre droit, y compris les conditions en matière constitutionnelle et de droits de l'homme, est respecté, tout particulièrement pour ce qui est des éventuelles garanties supplémentaires, y compris celles qui sont nécessaires en matière de production des données relatives au trafic.

130. Il existe certes diverses manières d'appliquer cet article, et une Partie peut souhaiter concevoir ses propres processus internes en y intégrant la flexibilité nécessaire pour traiter les demandes émanant de toute une série d'autorités compétentes diverses. Le paragraphe 3.b a été négocié pour garantir que la Partie requise se voie fournir suffisamment d'informations pour qu'un examen complet puisse être mené au besoin, car certaines Parties ont indiqué qu'elles émettraient leurs propres injonctions pour donner effet à celle de la Partie requise.

Paragraphe 3

131. Pour déclencher auprès de la Partie requise le processus qui donnera effet à l'injonction, la Partie requérante transmet l'injonction et les informations à l'appui de cette dernière. Le paragraphe 3 décrit ce qu'une Partie requérante doit communiquer à la Partie requise pour que celle-ci donne

effet à l'injonction et enjoigne à un fournisseur de service sur son territoire de produire les éléments demandés. Le paragraphe 3.a décrit les informations devant figurer dans l'injonction elle-même et inclut des informations fondamentales pour l'exécution de l'injonction. Les informations visées par le paragraphe 3.b, uniquement à l'usage de la Partie requise et qui ne doivent pas être communiquées avec le fournisseur de services sauf sur autorisation de la Partie requérante, sont des informations en appui à l'injonction qui posent dans le présent Protocole la base juridique nationale et internationale pour l'injonction, et sert à la Partie requise pour évaluer les motifs potentiels d'une réponse conditionnelle ou d'un refus en vertu du paragraphe 8. Lorsqu'elles envoient une demande en vertu de l'article 8, les Parties devraient indiquer si des informations relevant du paragraphe 3.b peuvent être partagées avec le fournisseur de services. En vertu du paragraphe 3.c, la demande devrait aussi, au moment de sa transmission et afin de garantir le traitement correct de la demande, inclure toutes instructions spéciales, par exemple des demandes pour une certification ou de confidentialité de la demande (de façon analogue à l'article 27, paragraphe 8, de la Convention).

132. L'injonction de produire des informations concernant l'abonné ou des données concernant le trafic, décrite au paragraphe 3.a, doit, sur sa première page, (i) préciser l'autorité qui a émis l'injonction et la date à laquelle cette injonction a été émise ; (ii) indiquer qu'elle est émise en vertu du présent Protocole ; (iii) indiquer le nom et l'adresse du ou des fournisseurs de services à notifier ; (iv) indiquer le ou les infractions faisant l'objet de l'enquête ou de la procédure pénale ; (v) indiquer l'autorité qui recherche les données, si ce n'est pas l'autorité émettrice ; et (vi) fournir une description détaillée des données spécifiques recherchées, autrement dit l'identité de l'abonné, l'adresse postale ou géographique, le numéro de téléphone ou autre numéro d'accès ainsi que les informations relatives à la facturation et au règlement disponibles du fait du contrat ou des modalités de service (voir l'article 3 du présent Protocole incorporant l'article 18, paragraphe 3, de la Convention et le paragraphe 93 du présent rapport explicatif) ; et pour ce qui est des données relatives au trafic, les données informatiques concernant une communication au moyen d'un système informatique, générées par un système informatique qui faisait partie de la chaîne de communication indiquant l'origine, la destination, le routage, l'heure, la date, la taille, la durée ou le type de services sous-jacent (voir l'article 3, paragraphe 1 du présent Protocole incorporant l'article 1, paragraphe d, de la Convention). En vertu du paragraphe 3.a.v, si l'autorité émettrice et celle qui demande les données sont différentes, en vertu de la disposition, les deux doivent être identifiées. Ainsi, une autorité d'enquête

ou de poursuite peut être celle qui demande les données et un juge celui qui émet l'injonction. Ces informations viennent à l'appui de la légitimité de l'injonction et de la clarté des instructions pour son exécution.

133. Les informations en appui décrites au paragraphe 3.b ont pour but de communiquer à la Partie requise les informations dont elle a besoin pour donner effet à l'injonction de la Partie requérante. Il serait également possible de faciliter leur communication en recourant à un formulaire facile à remplir qui rendrait le processus encore plus efficient et recueillerait notamment les éléments suivants:

- au titre du paragraphe 3.b.i, la base légale qui donne compétence à l'autorité émettrice pour émettre l'injonction visant l'obligation de produire les données demandées. En d'autres termes, cette rubrique comprendra la loi pertinente qui donne pouvoir à une autorité compétente pour émettre l'injonction décrite au paragraphe 1 ;
- au titre du paragraphe 3.b.ii, la disposition juridique concernant l'infraction mentionnée dans l'injonction telle que visée au paragraphe 3.a.iv et le barème de sanctions qui lui est associé. L'inclusion de ces deux éléments est importante pour que la Partie requise détermine si la demande entre dans le périmètre de ses obligations ;
- au titre du paragraphe 3.b.iii, toutes informations pouvant être fournies par la Partie requérante qui l'ont amenée à conclure que le ou les fournisseurs de services visés par l'injonction sont en possession des informations ou données demandées ou en ont le contrôle. Ces informations sont fondamentales pour démarrer le processus dans la Partie requise. L'identification du fournisseur national de services et le fait de penser que celui-ci possède ou contrôle les informations ou données requises est souvent une condition préalable à l'émission d'une demande d'injonction de produire ;
- au titre du paragraphe 3.b.iv, un bref résumé des faits liés à l'enquête ou à la procédure. Ces informations sont également essentielles pour que la Partie requise détermine s'il convient ou non de donner effet à une injonction sur son territoire ;
- au titre du paragraphe 3.b.v, une déclaration concernant la pertinence des informations ou données pour l'enquête ou la procédure. Cette déclaration est destinée à aider la Partie requise à décider si les conditions prévues au paragraphe 1 de l'article 8 sont remplies, autrement dit si les informations ou données sont « nécessaires pour les enquêtes ou procédures pénales spécifiques de la Partie requérante » ;

- au titre du paragraphe 3.b.vi, les coordonnées de contact d'une ou de plusieurs autorités si l'autorité compétente dans la Partie requise a besoin d'informations supplémentaires pour donner effet à l'injonction ;
- au titre du paragraphe 3.b.vii, des précisions concernant l'éventualité que la conservation des informations ou données a déjà été demandée. Cette information est importante pour la Partie requise, en particulier pour ce qui concerne les données liées au trafic, et devrait préciser, par exemple, les références de la demande et la date de la conservation, car elle permet à la Partie requise de rapprocher la demande nouvellement reçue d'une demande antérieure de conservation, et ainsi de faciliter la communication des informations ou données conservées à l'origine. Pour réduire le risque que des informations ou données soient effacées, les Parties sont encouragées à demander au plus tôt la conservation des informations ou données recherchées et de le faire avant d'intenter une demande en vertu du présent article, ainsi que de veiller à ce que l'extension de la préservation soit demandée en temps opportun ;
- au titre du paragraphe 3.b.viii, des précisions sur l'éventualité que les données aient déjà été demandées par d'autres moyens et si c'est le cas, comment. Cette disposition concerne essentiellement le cas où une Partie requérante a déjà sollicité directement auprès du fournisseur de service des informations relatives à l'abonné ou des données relatives au trafic.

134. Les informations à fournir en vertu du paragraphe 3.b ne sont pas communiquées au fournisseur de services sans l'accord de la Partie requérante. En particulier, le résumé des faits et la déclaration concernant la pertinence des informations ou les données pour l'enquête ou les poursuites sont communiqués à la Partie requise pour déterminer s'il y a lieu d'imposer des termes ou conditions, ou de refuser, mais cela relève souvent du secret de l'enquête.

135. En vertu du paragraphe 3.c, la Partie requérante peut demander des instructions procédurales spécifiques, dont des demandes de non-divulgateion de l'injonction à l'abonné ou des formulaires d'authentification à remplir pour la preuve. Ces informations doivent être connues dès le départ, étant donné que certaines instructions spéciales peuvent entraîner des processus supplémentaires chez la Partie requise.

136. Pour donner effet à l'injonction et pour faciliter davantage la production des informations et données, la Partie requise peut communiquer au

fournisseur de services des informations complémentaires telles que la méthode de production ou le destinataire de la production des données chez la Partie requise.

Paragraphe 4

137. En vertu du paragraphe 4, il peut être nécessaire de fournir des informations complémentaires à la Partie requise pour donner effet à l'injonction. Ainsi, dans le droit interne de certaines Parties, la production de données sur le trafic peut exiger la communication d'informations supplémentaires du fait de conditions supplémentaires dans ce droit pour l'obtention de ces données. De plus, la Partie requise peut demander des éclaircissements concernant les informations fournies en vertu du paragraphe 3.b ou encore des Parties peuvent demander des informations supplémentaires lorsque l'injonction n'a pas été émise ou revue par un procureur ou une autre autorité administrative judiciaire ou indépendante de la Partie requérante. Les Parties qui feront ce type de déclaration devraient être aussi spécifiques que possible pour ce qui concerne le type d'informations complémentaires requises.

Paragraphe 5

138. Le paragraphe 5 exige que la Partie requise accepte les demandes sous forme électronique. Il peut exiger l'utilisation de moyens de communication électroniques sûrs et authentifiables pour faciliter la transmission d'informations ou de données et de documents, y compris la transmission d'ordonnances et de renseignements à l'appui. Les articles 6 à 11 prévoient également de tels moyens de communication.

Paragraphe 6

139. En vertu du paragraphe 6, la Partie requise devrait prendre des mesures pour traiter rapidement la demande. Elle fait des efforts raisonnables pour traiter les demandes et notifier le fournisseur de services dans les 45 jours suivant sa réception de tous les documents et informations nécessaires. La Partie requise ordonnera au fournisseur de services de produire les informations relatives à l'abonné dans les 20 jours et les données relatives au trafic dans les 45 jours. La Partie requise devrait certes s'efforcer d'obtenir la production aussi rapidement que possible, toutefois de nombreux facteurs peuvent retarder celle-ci, par exemple les objections des fournisseurs de services, le fait que ces derniers ne répondent pas aux demandes ou ne respectent pas les délais pour la production, mais aussi le volume de demandes qu'une Partie requise peut se voir demander de traiter. Il a donc été décidé d'exiger que les Parties

requis fassent des efforts raisonnables pour mener à bien uniquement les processus sous leur contrôle.

Paragraphe 7

140. Les Parties ont reconnu que certaines instructions procédurales spéciales demandées par la Partie requérante pouvaient aussi causer des retards dans le traitement des injonctions, si les instructions requièrent des processus nationaux supplémentaires pour donner effet aux instructions procédurales spéciales. La Partie requise peut aussi demander des informations supplémentaires à la Partie requérante pour étayer toutes demandes d'injonctions supplémentaires telles que des injonctions de confidentialité (injonctions de non-divulgaration). Certaines instructions procédurales peuvent ne pas être prévues dans le droit de la Partie requise, auquel cas le paragraphe 7 prévoit que celle-ci en informe rapidement la Partie requérante et spécifie les conditions dans lesquelles elle pourrait donner suite à la demande, ce qui permet alors à la Partie requérante de déterminer si elle souhaite ou non poursuivre avec sa demande.

Paragraphe 8

141. En vertu du paragraphe 8, la Partie requise peut refuser d'exécuter une requête si les motifs de refus établis aux articles 25, paragraphe 4, ou 27, paragraphe 4, de la Convention existent. Par exemple, conformément au paragraphe 257 du rapport explicatif de la Convention, cette disposition est soumise aux motifs de refus prévus par les traités d'entraide judiciaire et les lois nationales applicables et offre « des garanties pour les droits des personnes se trouvant dans la Partie requise », et, conformément au paragraphe 268 de ce même rapport explicatif, l'entraide peut être refusée pour « atteinte à la souveraineté de l'État, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels ». Elle peut également imposer les conditions nécessaires pour permettre l'exécution de la demande, telles que la confidentialité. En outre, la Partie requise peut différer l'exécution de la requête en vertu de l'article 27, paragraphe 5, de la Convention. La Partie requise notifie à la Partie requérante sa décision de refuser, de conditionner ou de différer la demande. En outre, les Parties peuvent appliquer une limitation de l'usage conformément aux termes de l'article 28, paragraphe 2.b, de la Convention.

142. Afin de promouvoir le principe de la coopération la plus large possible (voir article 5, paragraphe 1), les motifs de refus établis par une Partie requise devraient être étroits et exercés avec retenue. Il convient de rappeler que le paragraphe 253 du rapport explicatif de la Convention prévoit que « l'entraide

doit en principe être étendue et les entraves dont elle peut faire l'objet doivent être strictement limitées ». En conséquence, les conditions et refus devraient également être limités conformément aux objectifs de cet article pour éliminer les obstacles au partage transfrontalier des informations relatives à l'abonné et des données relatives au trafic et pour mettre en place des procédures plus efficaces et rapides que l'entraide traditionnelle.

Paragraphe 9

143. En vertu du paragraphe 9, « a. [s]i la Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 8, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou le matériel doivent néanmoins être fournis. b. Si la Partie requérante accepte la condition, elle est liée par celle-ci. La partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ce matériel ».

Paragraphe 10

144. L'objet du paragraphe 10 est de faire en sorte que les Parties, au moment de la signature, ou au moment du dépôt de leurs instruments de ratification, d'acceptation ou d'approbation, identifient les autorités chargées de soumettre et de recevoir les injonctions en vertu de l'article 8. Les Parties ne sont pas tenues de donner le nom et l'adresse d'une personne en particulier, mais peuvent identifier un bureau ou une unité qui a été jugé compétent aux fins de l'envoi et de la réception des ordres en vertu de cet article.

Paragraphe 11

145. Le paragraphe 11 permet à une Partie de déclarer qu'elle demande que les injonctions qui lui sont soumises en vertu de cet article soient transmises par l'autorité centrale de la Partie requérante ou une autre autorité s'il en est ainsi convenu par les Parties. Les Parties sont encouragées à prévoir la plus grande souplesse pour la soumission de demandes.

Paragraphe 12

146. Le paragraphe 12 requiert que le Secrétaire Général ou la Secrétaire Générale du Conseil de l'Europe établisse et tienne à jour un registre des autorités désignées par les Parties en vertu du paragraphe 10 et que chaque Partie veille à ce que ses informations contenues dans le registre soient justes et

précises. Ces informations aideront les Parties requises à vérifier l'authenticité des demandes.

Paragraphe 13

147. En vertu du paragraphe 13, une Partie qui se réserve le droit de ne pas appliquer cet article aux données relatives au trafic n'est pas tenue de donner effet à des injonctions de production de données relatives au trafic émanant d'une autre Partie. Une Partie qui émet des réserves concernant cet article n'est pas autorisée à soumettre des injonctions de production de données relatives au trafic à d'autres Parties en vertu du paragraphe 1.

Article 9 – Divulgence rapide de données informatiques stockées en cas d'urgence

148. Outre les autres formes de coopération accélérée prévues par le Protocole, les rédacteurs étaient conscients de la nécessité de faciliter la capacité des Parties d'obtenir rapidement, dans une situation d'urgence spécifiée, des données informatiques stockées en possession ou sous le contrôle d'un fournisseur de services sur le territoire d'une autre Partie pour les utiliser dans le cadre d'enquêtes ou de procédures pénales spécifiques. Comme cela est indiqué aux paragraphes 42 et 172 du présent rapport explicatif, il peut être nécessaire de demander une coopération la plus rapide possible dans diverses situations où l'urgence est un facteur primordial, juste après une attaque terroriste par exemple, après une attaque par rançongiciel qui peut paralyser le système d'un hôpital, ou lors de l'enquête sur les comptes de messagerie utilisés par les ravisseurs pour faire connaître des exigences et communiquer avec la famille de la victime.

149. En vertu de la Convention, dans des situations d'urgence, les Parties font des demandes d'entraide pour obtenir des données et, en vertu de l'article 35, paragraphe 1.c, de la Convention, le Réseau 24/7 est disponible pour faciliter l'exécution de ces demandes. En outre, les systèmes juridiques de quelques pays permettent aux autorités compétentes d'autres pays de demander la divulgation d'urgence des données par l'intermédiaire du Réseau 24/7 sans envoyer de demande d'entraide.

150. Comme cela est indiqué à l'article 5, paragraphe 7, le présent article ne porte pas atteinte à la coopération (y compris spontanée) entre les Parties ou entre les Parties et les fournisseurs de services par le biais d'autres accords, arrangements, pratiques ou lois nationales applicables. Par conséquent, en vertu du présent Protocole, tous les mécanismes susmentionnés restent à

la disposition des autorités compétentes qui demandent des données en situation urgente. L'innovation du Protocole est l'élaboration de deux articles qui obligent toutes les Parties à fournir, au minimum, des voies spécifiques pour une coopération accélérée pouvant être activée rapidement dans les situations urgentes, à savoir l'article 9 et l'article 10.

151. L'article 9 permet aux Parties de coopérer pour obtenir des données informatiques dans des situations d'urgence en utilisant comme canal le Réseau 24/7 établi par l'article 35 de la Convention. Le Réseau 24/7 est particulièrement bien adapté pour traiter les demandes pour lesquelles le facteur temps est crucial et hautement prioritaire, qui sont prévues à l'article 9. Le Réseau 24/7 est doté de points de contact qui, dans la pratique, communiquent rapidement sans avoir besoin de traductions écrites et sont en mesure d'exécuter les demandes reçues d'autres Parties, que ce soit en allant directement auprès de fournisseurs sur leur territoire, en sollicitant l'aide d'autres autorités compétentes ou en s'adressant aux autorités judiciaires, si cette condition est prévue par le droit interne de la Partie. Ces points de contact peuvent également conseiller les Parties requérantes sur des questions qu'elles pourraient se poser concernant les fournisseurs et la collecte de preuves électroniques, par exemple, en expliquant le droit interne qui doit être satisfait pour obtenir des éléments de preuve. Cette communication en aller-retour améliore la compréhension par la Partie requérante du droit interne dans la Partie requise et permet un recueil plus facile des éléments de preuve nécessaires.

152. L'utilisation du canal prévu au présent article peut avoir des avantages par rapport au canal d'entraide judiciaire d'urgence énoncé à l'article 10. Par exemple, ce canal présente l'avantage de ne pas nécessiter la préparation à l'avance d'une demande d'entraide. Il faut parfois beaucoup de temps pour préparer au préalable une demande d'entraide, la faire traduire et la transmettre par les voies nationales à l'autorité centrale de la Partie requérante compétente en matière d'entraide, ce qui ne serait pas nécessaire en vertu de l'article 9. En outre, une fois que la Partie requise a reçu la demande, si elle doit obtenir des renseignements supplémentaires avant de pouvoir accorder une aide, le temps supplémentaire qui peut être nécessaire pour une demande d'entraide est susceptible de ralentir l'exécution de la demande. Dans le contexte de l'entraide, les Parties requises exigent souvent que les informations supplémentaires soient fournies sous une forme écrite et plus détaillée, alors que le canal 24/7 fonctionne par l'échange d'informations en temps réel. De plus, le canal de l'entraide judiciaire urgente offre des avantages

dans certaines situations. Par exemple: (i) on ne perd pas ou peu de temps en utilisant ce canal s'il existe des relations de travail particulièrement étroites entre les autorités centrales concernées ; (ii) l'entraide d'urgence peut être utilisée pour obtenir des formes supplémentaires de coopération au-delà des données informatiques détenues par les fournisseurs ; et (iii) il peut être plus facile d'authentifier les éléments de preuve obtenus par l'intermédiaire de l'entraide judiciaire. Il appartient aux Parties, sur la base de leur expérience et des circonstances juridiques et factuelles spécifiques en cause, de décider quel est le meilleur canal à utiliser dans un cas particulier.

Paragraphe 1

153. En vertu du paragraphe 1.a, chaque Partie adopte les mesures nécessaires pour s'assurer que son point de contact pour le Réseau 24/7 est en mesure de transmettre les demandes en cas d'urgence au point de contact d'une autre Partie demandant une assistance immédiate pour obtenir la divulgation accélérée des données informatiques spécifiées et stockées détenues par les fournisseurs sur le territoire de cette Partie et recevoir des demandes de points de contact dans d'autres Parties concernant lesdites données détenues par des fournisseurs sur son territoire. Comme le prévoit l'article 2, la demande doit être présentée dans le cadre d'une enquête ou procédure pénale spécifique.

154. Les points de contact du Réseau 24/7 doivent avoir la capacité de transmettre et de recevoir ces demandes en cas d'urgence sans qu'une demande d'entraide doive être préparée et transmise à l'avance comme cela est décrit au paragraphe 152 du présent rapport explicatif, sous réserve de la possibilité d'une déclaration au titre de l'article 9, paragraphe 5. Le terme « urgence » est défini à l'article 3. En vertu de l'article 9, la Partie requise devrait déterminer s'il existe une « urgence » par rapport à une demande en utilisant les informations fournies au paragraphe 3.

155. Contrairement à d'autres articles du présent Protocole, tels que l'article 7, qui ne peuvent être utilisés que pour obtenir des « informations relatives à l'abonné spécifiées et stockées », le présent article utilise l'expression plus large « données informatiques spécifiées et stockées ». Le champ d'application de cette expression est large mais il n'est pas générique: il couvre les données informatiques « spécifiées » telles que définies à l'article 1.b de la Convention, qui est repris à l'article 3, paragraphe 1, du présent Protocole. L'utilisation de cette expression plus large reconnaît l'importance d'obtenir du contenu stocké et des données de trafic, et pas uniquement des informations relatives à l'abonné, dans des situations d'urgence sans exiger la présentation d'une

demande d'entraide comme condition préalable. Les données en question sont stockées ou existantes et n'incluent pas de données qui n'existent pas encore, telles que les données de trafic ou les données de contenu relatives aux communications futures (voir le rapport explicatif de la Convention, paragraphe 170).

156. Cette disposition offre à la Partie requérante la latitude nécessaire pour déterminer quelles autorités devraient la présenter, par exemple ses autorités compétentes qui mènent l'enquête, ou le point de contact du Réseau 24/7, conformément au droit interne. Le point de contact du Réseau 24/7 de la Partie requérante fonctionne alors comme canal pour transmettre la demande au point de contact du Réseau 24/7 de l'autre Partie.

157. En vertu du paragraphe 1.b, une Partie peut déclarer qu'elle n'exécutera pas une demande en vertu de l'article 9 visant uniquement des informations relatives à l'abonné, telles que définies à l'article 18, paragraphe 3, de la Convention, incorporées à l'article 3, paragraphe 1, du présent Protocole. Pour certaines Parties, recevoir des demandes en vertu de l'article 9 uniquement pour des informations relatives aux abonnés risquerait de surcharger les points de contact du Réseau 24/7 en détournant les ressources et l'énergie des demandes de contenu ou de données relatives au trafic. Dans de tels cas, les Parties qui ne cherchent qu'à obtenir des informations sur les abonnés peuvent plutôt utiliser les articles 7 ou 8, qui facilitent la divulgation rapide de ces informations. Une telle déclaration n'interdit pas à d'autres Parties d'inclure une demande d'informations relatives aux abonnés lorsqu'elles émettent également une demande en vertu du présent article pour le contenu et/ou les données relatives au trafic.

Paragraphe 2

158. Le paragraphe 2 exige que chaque Partie adopte les mesures nécessaires pour que ses autorités soient habilitées, en vertu de son droit interne, à demander et à obtenir des données demandées en vertu du paragraphe 1 auprès des fournisseurs de services sur son territoire et à répondre à ces demandes sans que la Partie requérante n'ait à présenter une demande d'entraide, sous réserve de pouvoir faire une déclaration conformément au paragraphe 5.

159. Compte tenu des différences entre droits internes, le paragraphe 2 vise à donner aux Parties la souplesse nécessaire pour la construction de leurs systèmes de réponse aux demandes en vertu du paragraphe 1. Les Parties sont toutefois encouragées à élaborer des mécanismes conformes au présent

article qui mettent l'accent sur la rapidité et l'efficacité, sont adaptés aux exigences d'une situation d'urgence et donnent une base juridique générale pour la divulgation aux autres Parties de données dans les situations d'urgence.

160. Il appartient à la Partie requise de déterminer: 1. si les conditions permettant d'invoquer le présent article ont été remplies ; 2. si un autre mécanisme est approprié pour aider la Partie requérante ; 3. l'autorité compétente pour exécuter une demande reçue par le point de contact du Réseau 24/7. Bien que le point de contact du Réseau 24/7 de certaines Parties puisse déjà avoir la compétence requise pour exécuter la demande lui-même, d'autres Parties peuvent exiger que le point de contact transmette la demande à une ou d'autres autorités pour demander au fournisseur de divulguer les données. Dans certaines Parties, cela peut dépendre de l'obtention d'une ordonnance judiciaire pour demander la divulgation des données. La Partie requise a également tout pouvoir pour déterminer le canal à utiliser pour transmettre les données en réponse à la Partie requérante, que ce soit par l'intermédiaire du point de contact du Réseau 24/7 ou par l'intermédiaire d'une autre autorité.

Paragraphe 3

161. Le paragraphe 3 précise les informations à fournir dans une demande formulée en vertu du paragraphe 1. Les informations spécifiées au paragraphe 3 visent à faciliter l'examen et, le cas échéant, l'exécution de la demande par l'autorité compétente de la Partie requise.

162. En ce qui concerne le paragraphe 3.a, la Partie requérante précise l'autorité compétente au nom de laquelle les données sont demandées.

163. En ce qui concerne le paragraphe 3.b, la Partie requérante doit indiquer que la demande est émise conformément au présent Protocole. Cela permettra d'assurer que la demande est faite conformément au Protocole et que toutes les données reçues en conséquence seront traitées d'une manière conforme aux exigences du Protocole. Cela permettra également de différencier la demande des autres demandes de divulgation d'urgence que le point de contact du Réseau 24/7 pourrait recevoir.

164. En application du paragraphe 3.e, la Partie requérante doit communiquer suffisamment de faits à l'appui de l'existence d'une situation urgente, telle que définie à l'article 3, et expliquer comment les données recherchées par la demande se rapportent à ladite situation. Si la Partie requise a besoin d'éclaircissements sur la demande ou exige des informations supplémentaires

pour donner suite à la demande, elle devrait consulter le point de contact du Réseau 24/7 de la Partie requérante.

165. En application du paragraphe 3.g, la demande précise toute instruction procédurale spéciale. Il s'agit notamment des demandes particulières de non-divulgence de la demande aux abonnés et autres tiers ou des formulaires d'authentification à remplir pour les données recherchées. En vertu de ce paragraphe, ces instructions de procédure sont fournies dès le départ, car des instructions spéciales peuvent entraîner des processus supplémentaires chez la Partie requise. Dans certaines Parties, la confidentialité peut être préservée par application de la loi, alors que dans d'autres Parties ce n'est pas nécessairement le cas. Par conséquent, afin d'éviter le risque de divulgation prématurée de l'enquête, les Parties sont encouragées à communiquer sur la nécessité de préserver la confidentialité et les difficultés qui pourraient se poser, préciser les éventuelles lois applicables, ainsi que les politiques d'un fournisseur de services concernant la notification. Étant donné que les demandes d'authentification des données en réponse à une demande peuvent souvent ralentir le processus alors que l'objectif clé est la divulgation rapide des données recherchées, les autorités de la Partie requise devraient déterminer, en consultation avec les autorités de la Partie requérante, quand et de quelle manière la confirmation de l'authenticité doit être donnée.

166. En outre, la Partie ou le fournisseur de services peut exiger des informations supplémentaires pour localiser et divulguer les données informatiques stockées recherchées par la Partie requérante.

Paragraphe 4

167. Le paragraphe 4 exige que la Partie requise accepte les demandes sous forme électronique. Les Parties sont encouragées à utiliser des moyens de communication rapides pour faciliter la transmission d'informations ou de données et de documents, y compris la transmission des demandes. Ce paragraphe est fondé sur le paragraphe 5 de l'article 8 mais il a été modifié pour ajouter qu'une Partie peut accepter des demandes oralement, une méthode de communication fréquemment utilisée par le Réseau 24/7.

Paragraphe 5

168. Le paragraphe 5 permet à une Partie de déclarer qu'elle exige que d'autres Parties qui lui demandent des données conformément au présent article fournissent, après l'exécution de la demande et transmission des données, la demande et toute information supplémentaire transmise à l'appui de

celle-ci, dans un format spécifique et par le biais d'un canal spécifique. Par exemple, une Partie peut déclarer que, dans des circonstances spécifiques, elle demandera à une Partie requérante que cette dernière soumette subséquemment une demande d'entraide judiciaire afin de justifier formellement la demande d'urgence la décision préalable de fournir des données en réponse à une telle demande. Pour certaines Parties, une telle procédure serait exigée par leurs lois nationales, tandis que d'autres Parties ont indiqué qu'elles n'ont pas de conditions de ce type et n'ont pas à se prévaloir de cette possibilité de déclaration.

Paragraphe 6

169. Le présent article fait référence à des « demandes » et n'exige pas que les Parties requises fournissent les données demandées aux Parties requérantes. Par conséquent, les rédacteurs reconnaissent qu'il y aura des situations dans lesquelles les Parties requises ne fourniront pas les données demandées à une Partie requérante en vertu du présent article. La Partie requise peut déterminer que, dans un cas particulier, une entraide d'urgence en vertu de l'article 10 ou un autre moyen de coopération serait le plus approprié. Par conséquent, le paragraphe 6 prévoit que lorsqu'une Partie requise détermine qu'elle ne fournira pas les données demandées à une Partie qui a fait une demande en vertu du paragraphe 1 du présent article, la Partie requise informe la Partie requérante de sa décision rapidement et, le cas échéant, précise les conditions dans lesquelles elle fournirait les données et explique toute autre forme de coopération qui pourrait être disponible, afin d'atteindre l'objectif mutuel des Parties d'accélérer la divulgation des données en cas d'urgence.

Paragraphe 7

170. Le paragraphe 7 décrit les procédures applicables lorsque l'État requis a spécifié les conditions dans lesquelles il accède à la demande de coopération qui lui a été adressée en vertu du paragraphe 6. Si la partie requérante ne peut pas se conformer à ces conditions, le paragraphe 7.a lui impose d'en informer rapidement la Partie requise, qui décidera alors si l'assistance demandée peut tout de même être accordée. En revanche, lorsque la Partie requérante accepte une condition spécifique, elle est tenue de la respecter. En vertu du paragraphe 7.b, une Partie requise qui a transmis des renseignements ou du matériel sous réserve d'une condition fixée en application du paragraphe 6 peut, afin de pouvoir contrôler le respect de cette condition, exiger que la Partie requérante explique l'usage qui a été fait des renseignements ou du matériel transmis, mais il a été entendu que

la Partie requérante ne pouvait pas exiger une comptabilité trop lourde (voir rapport explicatif de la Convention, paragraphes 279 et 280).

Section 4 – Procédures relatives à l’entraide d’urgence

Article 10 – Entraide d’urgence

171. L’article 10 du Protocole a pour but de prévoir une procédure qui soit rapide pour les demandes d’entraide effectuées en situation d’urgence. Une situation d’urgence est définie à l’article 3, paragraphe 2.c, et expliquée dans les paragraphes correspondants 41 et 42 du présent rapport explicatif.

172. Étant donné que l’article 10 de ce Protocole est limité aux urgences justifiant une telle célérité dans l’action, il est distinct de l’article 25, paragraphe 3, de la Convention, qui prévoit que les demandes d’entraide peuvent être transmises par des moyens de communication rapides en situations d’urgence qui ne sont pas du niveau d’urgence défini. En d’autres termes, l’article 25, paragraphe 3, a une portée plus large que l’article 10 du Protocole puisqu’il couvre des situations non couvertes par ce dernier, par exemple les risques existants mais non imminents pour la vie ou la sécurité de personnes physiques, la destruction potentielle de preuves qui pourrait résulter d’un retard, le fait que la date d’un procès se rapproche ou autres types d’urgences. Alors que le mécanisme visé à l’article 25, paragraphe 3, prévoit une méthode plus rapide pour transmettre une demande et y répondre, les obligations en cas d’urgence relevant de l’article 10 du Protocole sont nettement plus lourdes ; en d’autres termes, lorsqu’il existe un risque significatif et imminent pour la vie ou la sécurité d’une personne physique, le processus devrait être encore plus rapide (voir paragraphe 42 du présent rapport explicatif pour des exemples de situations d’urgence).

Paragraphe 1

173. En vertu du paragraphe 1, lorsqu’elle présente une demande d’urgence, la Partie requérante doit à la fois conclure qu’il existe une urgence au sens de l’article 3, paragraphe 2.c, et inclure dans sa demande une description des faits tendant à le démontrer et expliquer comment l’entraide sollicitée est nécessaire pour répondre à la situation urgente, en plus des informations qui doivent figurer dans la demande en vertu du traité applicable ou du droit interne de la Partie requise. À cet égard, il convient de rappeler qu’au titre de l’article 25, paragraphe 4, de la Convention l’exécution des demandes d’entraide judiciaire, y compris urgentes, est en général « soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d’entraide applicables, y compris

les motifs sur la base desquels la Partie requise peut refuser la coopération ». Les rédacteurs considéraient que cela s'appliquait également aux demandes d'entraide d'urgence au titre du présent protocole.

Paragraphe 2

174. Le paragraphe 2 exige de la Partie requise qu'elle accepte la demande d'entraide sous forme électronique. Avant d'accepter la demande, la Partie requise peut conditionner son acceptation au respect par la Partie requérante de niveaux de sécurité et d'authentification appropriés. Pour ce qui est de la condition de sécurité prévue dans ce paragraphe, les Parties peuvent décider d'un commun accord s'il est nécessaire d'établir des protections de sécurité spéciales (dont le cryptage) en cas d'affaire particulièrement sensible.

Paragraphe 3

175. Lorsque la Partie requise demande un complément d'informations pour étayer la situation urgente au sens de l'article 3, paragraphe 2.c, et/ou que les autres conditions liées à la demande d'entraide ont été remplies, le paragraphe 3 prévoit que ce complément d'informations doit être demandé de manière accélérée. De même, le paragraphe 3 exige de la Partie requérante qu'elle communique le complément d'informations avec la même célérité. Les deux Parties devraient donc faire leur maximum pour éviter toute perte de temps qui pourrait involontairement entraîner une issue tragique.

Paragraphe 4

176. En vertu du paragraphe 4, une fois que les informations nécessaires à l'exécution de la demande ont été communiquées, il est demandé à la Partie requise d'exécuter la demande urgente avec la même célérité. En général, cela signifie le fait d'obtenir d'urgence les mandats judiciaires obligeant le fournisseur à produire les données qui prouvent l'infraction et de faire procéder d'urgence à la signification toute aussi rapide de l'injonction au fournisseur. Cependant, les autorités de la Partie requise ne sauraient être tenues responsables des retards occasionnés par les délais de réponse du fournisseur à ces injonctions.

Paragraphe 5

177. En vertu du paragraphe 5, toutes les Parties veillent à ce que des membres de leur autorité centrale ou d'autres autorités responsables des demandes d'entraide soient joignables 24 heures sur 24, sept jours sur sept, pour recevoir des demandes d'entraide urgentes qui parviendraient en dehors des heures

ouvrables. Il convient de rappeler qu'à cet égard, le Réseau 24/7 créé au titre de l'article 35 de la Convention est disponible pour se coordonner avec les autorités responsables de l'entraide. L'obligation prévue dans ce paragraphe n'exige pas de l'autorité centrale ou des autres autorités responsables des demandes d'entraide qu'elle(s) prévoie(nt) un personnel dédié et opérationnel à tout moment. En revanche, elle devrait prendre des mesures pour garantir que des membres de son personnel sont joignables en dehors des heures ouvrables pour examiner des demandes urgentes. Le T-CY s'efforcera de manière informelle de tenir un répertoire de ces autorités.

Paragraphe 6

178. Le paragraphe 6 offre une base qui permet aux autorités centrales et aux autres autorités responsables de l'entraide de s'entendre sur un canal alternatif de transmission des informations demandées ou de la preuve ; il peut s'agir du mode de transmission ou des autorités entre lesquelles s'opère la transmission. Ainsi, plutôt que de renvoyer les informations ou preuves demandées par le biais de l'autorité centrale habituellement utilisée pour la transmission des informations prévues ou des preuves aux fins de l'exécution de la demande par la Partie requérante, elles peuvent alors décider d'utiliser un canal différent pour accélérer la transmission, préserver l'intégrité de la preuve ou pour toute autre raison. Par exemple, en cas d'urgence, les autorités peuvent décider de la transmission des preuves directement à une autorité d'enquête ou de poursuite de la Partie requérante qui les utilisera, plutôt que de les transmettre via la chaîne des autorités qui se chargent en temps normal de les acheminer. Les autorités peuvent aussi, par exemple, déterminer un traitement spécial de preuves matérielles pour être à même d'écarter dans les procédures judiciaires ultérieures les contestations au motif que la preuve aurait pu avoir été altérée ou contaminée, ou peuvent décider ensemble d'un traitement spécial de la transmission de preuves sensibles.

Paragraphe 7

179. S'agissant des procédures visées à cet article, il existe deux possibilités, décrites aux paragraphes 7 et 8 de l'article 10. Le paragraphe 7 dispose que les Parties concernées, lorsqu'elles ne sont pas liées par un accord d'entraide en vigueur, ou par un accord applicable sur la base d'une législation uniforme ou réciproque, appliquent certaines procédures définies aux paragraphes visés des articles 27 et 28 de la Convention (régissant l'entraide en l'absence d'un traité).

Paragraphe 8

180. En vertu du paragraphe 8, lorsque les Parties concernées sont liées par un tel accord ou arrangement, l'article 10 est complétée par les dispositions de cet accord ou de cet arrangement, à moins que les Parties concernées décident d'un commun accord d'appliquer tout ou partie des dispositions de la Convention visées au paragraphe 7 en lieu et place dudit accord.

Paragraphe 9

181. Enfin, le paragraphe 9 prévoit la possibilité d'une déclaration par laquelle les Parties au présent Protocole peuvent prévoir que les demandes peuvent être faites directement entre les procureurs ou autres autorités judiciaires. Dans certaines Parties, ces voies de communication directes entre autorités judiciaires sont bien établies et peuvent constituer un moyen efficace d'accélérer encore la présentation et l'exécution des demandes. La transmission de la demande d'urgence par le point de contact de la Partie 24 heures sur 24 et sept jours sur sept ou par l'Organisation internationale de police criminelle (Interpol) est utile non seulement pour réduire tout retard mais aussi pour renforcer les normes de sécurité et d'authentification. Toutefois, dans certaines Parties, l'envoi d'une demande directement à une autorité judiciaire de la Partie requise sans l'intervention et l'approbation de son autorité centrale pourrait être contre-productif dans la mesure où, sans les conseils et/ou l'approbation de l'autorité centrale, l'autorité destinataire peut ne pas être habilitée à agir de manière indépendante, ou peut ne pas être familiarisée avec la procédure appropriée. Par conséquent, une partie doit déclarer que les demandes peuvent être envoyées par ces canaux d'autorité non centrale.

Section 5 – Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

182. Comme le prévoit l'article 5, paragraphe 5, la section 5, relative aux articles 11 et 12, s'applique « lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les Parties requérante et requise. Les dispositions de la section 5 ne s'appliquent pas lorsqu'un tel traité ou arrangement existe, sauf dans les cas prévus à l'article 12, paragraphe 7. Toutefois, les Parties concernées peuvent décider d'un commun accord d'appliquer la section 5 en lieu et place de celle-ci, si le traité ou l'arrangement ne l'interdit pas ». Cela suit l'approche de l'article 27 de la Convention.

183. Entre certaines Parties à ce Protocole, les sujets des articles 11 et 12 sont déjà réglementés par les termes des traités d'entraide (par exemple, le Deuxième Protocole STE no 182 ; ou l'Accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique). D'autres traités d'entraide, tels que le Deuxième Protocole STE no 182, peuvent également fournir plus de détails sur les circonstances dans lesquelles une telle coopération peut avoir lieu, ainsi que sur les conditions et les procédures qui la régissent.

184. Bien que les rédacteurs aient examiné ces traités, les articles 11 et 12 du présent Protocole contiennent des termes qui diffèrent des dispositions analogues figurant dans d'autres traités d'entraide.

185. Bien que les termes du Deuxième Protocole STE no 182 continueront à être appliqués entre les Parties à celle-ci, il a été jugé approprié de réglementer ces deux articles dans le présent Protocole d'une manière qui diffère à certains égards pour les raisons suivantes:

- la composition du Deuxième Protocole STE no 182 est différente de celle de la Convention sur la cybercriminalité et ses dispositions ne sont donc pas disponibles pour la coopération entre toutes les Parties à la Convention sur la cybercriminalité. Le Deuxième Protocole STE no 182 a été négocié pour répondre aux besoins des États membres du Conseil de l'Europe plutôt qu'aux exigences, systèmes et besoins juridiques de toutes les Parties à la Convention sur la cybercriminalité, bien que, en principe, la Convention européenne d'entraide judiciaire en matière pénale (STE n° 30) et ses Protocoles soient ouverts à l'adhésion des États non-membres du Conseil de l'Europe à la suite d'une invitation du Comité des Ministres ;
- les dispositions du présent Protocole relatives à l'entraide judiciaire ont un champ d'application matériel spécifique en ce sens qu'elles s'appliquent aux « enquêtes ou procédures pénales spécifiques concernant les infractions pénales liées aux systèmes et données informatiques, ainsi qu'à la collecte de preuves sous forme électronique d'une infraction pénale » (article 2). Compte tenu des problèmes particuliers de ce type d'enquêtes ou de procédures – tels que la volatilité des données, les questions liées à la territorialité et à la compétence, et au volume des demandes – les dispositions analogues du Deuxième Protocole STE no 182 ne sont pas toujours applicables de la même manière ;
- les rédacteurs ont reconnu que « puisque la Convention s'applique à des Parties ayant des systèmes juridiques et des cultures très différents, il n'est pas possible de préciser en détail les conditions et les garanties

applicables à chaque pouvoir ou procédure » (voir paragraphe 145 du rapport explicatif de la Convention). En revanche, les Parties sont tenues de veiller à assurer « une protection adéquate des droits de l'homme et des libertés » et à appliquer « des normes communes [et] des garanties minimales auxquelles les Parties [...] doivent adhérer », y compris « les garanties découlant des obligations qu'une Partie a contractées en vertu des instruments internationaux relatifs aux droits de l'homme applicables » (voir le rapport explicatif, paragraphe 145, de la Convention ; voir l'article 13 du présent Protocole – incorporant l'article 15 de la Convention). Par conséquent, contrairement aux dispositions du Deuxième Protocole STE no 182 – par exemple, l'article 9 sur l'« audition par vidéoconférence » – qui prescrivent des procédures et des garanties spécifiques à suivre par les Parties au Deuxième Protocole STE no 182, les dispositions correspondantes du présent Protocole permettent une plus grande souplesse dans la mise en œuvre par les Parties. Par exemple, les procédures et conditions régissant le fonctionnement des équipes communes d'enquête doivent être convenues entre les autorités compétentes des Parties (voir article 12, paragraphe 2), et, en ce qui concerne la vidéoconférence, une Partie requise peut exiger des conditions et garanties particulières lorsqu'elle autorise l'audition d'un suspect ou d'une personne poursuivie par vidéoconférence (voir article 11, paragraphe 7). Dans la mesure prévue par ces articles, les Parties peuvent également décider de ne pas coopérer si leurs exigences en matière de conditions et de garanties ne sont pas satisfaites.

186. Les articles 11 et 12 du présent Protocole ne s'appliquent qu'en l'absence d'autres traités ou arrangements d'entraide sur la base de législations uniformes ou réciproques – à moins que les parties concernées ne décident d'un commun accord d'appliquer tout ou partie de leurs dispositions à la place de celles-ci, si le traité ou l'arrangement ne l'interdit pas. Toutefois, l'article 12, paragraphe 7, s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les parties concernées.

Article 11 – Vidéoconférence

187. L'article 11 concerne avant tout le recours à la technologie de la vidéoconférence pour recueillir des témoignages ou des dépositions. Cette forme de coopération peut être prévue dans des traités d'entraide judiciaire bilatéraux et multilatéraux, par exemple dans le Deuxième Protocole STE no 182. Pour ne pas se substituer à des dispositions spécifiquement conçues pour répondre aux

besoins des parties à ces traités ou conventions, et comme indiqué dans les principes généraux applicables à la présente section (article 5, paragraphe 5), l'article 11, comme l'article 12 du présent Protocole « s'applique en l'absence de traité sur l'entraide judiciaire, ou d'arrangements sur la base de l'uniformité ou de la réciprocité législatives, en vigueur entre les Parties requérante et requise. Les dispositions de la section 5 ne sont pas applicables lorsqu'un tel traité ou arrangement existe, sauf dans les cas prévus à l'article 12, paragraphe 7. Toutefois, les parties concernées peuvent convenir de déterminer d'un commun accord d'appliquer les dispositions de la section 5 en lieu et place de celles-ci, si le traité ou l'arrangement ne l'interdit pas ».

Paragraphe 1

188. Le paragraphe 1 autorise le recueil de témoignages ou de dépositions d'un témoin ou expert par le recours à la vidéoconférence. Il laisse à la Partie requise toute latitude pour accepter ou non la demande d'entraide ou pour fixer des conditions à son assistance. Par exemple, une Partie peut refuser de fournir, ou remettre à plus tard, une assistance pour les motifs prévus à l'article 27, paragraphes 4 et 5, de la Convention. Par ailleurs, s'il est plus efficace que l'assistance soit fournie d'une manière différente, par exemple au moyen d'un formulaire écrit authentifiant des documents officiels ou commerciaux, la Partie requise peut choisir de fournir l'assistance de cette manière.

189. Dans le même temps, il est attendu des Parties au Protocole qu'elles disposent de la capacité technique de base pour exécuter la demande d'entraide au moyen de la vidéoconférence.

190. Utiliser la vidéoconférence pour recueillir un témoignage ou une déposition peut poser de nombreuses difficultés, notamment de nature juridique, logistique ou technique. Pour que la vidéoconférence fonctionne sans heurts, il est essentiel de se coordonner par avance. Parfois, durant l'opération, si la Partie requise pose des conditions préalables à la vidéoconférence, une coordination supplémentaire peut être nécessaire. Le paragraphe 1 exige donc aussi que les Parties requérante et requise se concertent au besoin pour faciliter la résolution de tout problème de ce type qui pourrait se poser. Par exemple, comme expliqué plus avant, la vidéoconférence peut devoir suivre une certaine procédure pour que les éléments recueillis soient admissibles en tant que preuve devant les juridictions de la Partie requérante. Il se peut aussi que la Partie requise ait besoin d'appliquer ses propres conditions juridiques à certains égards (par exemple pour une prestation de serment du témoin ou la notification de ses droits à ce dernier). De plus, la Partie requise peut exiger que son ou ses représentants des services concernés soient présents à la vidéoconférence dans certains ou

dans tous les cas, qu'ils puissent contrôler la procédure ou veiller à ce que les droits de la personne dont on recueille le témoignage ou la déposition soient respectés. À cet égard, il peut ressortir des consultations que certaines Parties requises exigent que leur représentant à la vidéoconférence puisse intervenir, interrompre ou mettre un terme à l'audition s'il y a des doutes quant à la conformité avec les dispositions de son droit interne, alors que d'autres Parties peuvent autoriser la tenue d'une vidéoconférence sans participation d'un représentant dans certains cas. Autre exemple, des Parties requises peuvent envisager des garanties spécifiques concernant les témoins menacés, les enfants témoins, etc. Ces questions doivent être discutées et décidées à l'avance. Dans certains cas, le souhait de la Partie requise de mener une seule procédure peut aller à l'encontre des dispositions légales de la Partie requérante ayant pour objectif de faciliter l'utilisation du témoignage ou de la déposition durant le procès. En de tels cas, les Parties devraient faire leur maximum pour tenter de trouver des solutions créatives répondant aux impératifs de chacune. De plus, les Parties doivent se consulter à l'avance pour faciliter la résolution des problèmes tels que la manière de répondre aux objections ou revendications de privilège ou d'immunité de la part de la personne concernée ou de son avocat, ou encore la manière d'utiliser des preuves documentaires ou autres durant la vidéoconférence. Il est aussi possible que des procédures particulières soient nécessaires du fait de conditions posées à la tenue de la vidéoconférence. Des questions logistiques, par exemple savoir qui, de la Partie requérante ou de la Partie requise, devrait assurer l'interprétation et l'enregistrement du témoignage ou de la déposition, devraient aussi être discutées ; la coordination technique devrait aussi être abordée pour régler les modalités relatives au démarrage et au maintien de la transmission, ainsi que pour disposer de canaux alternatifs de communication si la transmission est interrompue.

Paragraphe 2

191. Le paragraphe 2 traite de plusieurs aspects d'ordre procédural et apparenté régissant cette forme de coopération (outre les autres procédures et conditions applicables exposées dans les autres paragraphes de cet article), qui ont été repris ou adaptés de la Convention. Le paragraphe 2 se subdivise en deux sous-paragraphes.

192. La vidéoconférence constituant une forme d'entraide, le paragraphe 2.a dispose que les autorités centrales des Parties requises et requérantes communiquent directement entre elles aux fins de l'application de cet article. Cet article s'appliquant uniquement en l'absence d'un accord ou d'un arrangement d'entraide sur la base d'une législation uniforme ou réciproque, on entend

ici par « autorité centrale » l'autorité ou les autorités désignées en vertu de l'article 27, paragraphe 2.a, de la Convention (voir l'article 3, paragraphe 2.a, et le paragraphe 38 du rapport explicatif de la Convention).

193. Le paragraphe 2.a de cet article prévoit aussi qu'une Partie requise accepte une requête de vidéoconférence sous forme électronique et qu'elle puisse exiger des niveaux de sécurité et d'authentification appropriés avant d'accepter cette demande.

194. Le paragraphe 2.b (de même que l'article 27, paragraphe 7, de la Convention) impose à la Partie requise d'informer la Partie requérante des raisons pour lesquelles elle n'a pas exécuté la demande ou tardé à l'exécuter. Comme cela est indiqué au paragraphe 192 ci-dessus, ces communications doivent passer par des autorités centrales. Enfin, le paragraphe 2.b prévoit que l'article 27, paragraphe 8 (relatif à la confidentialité d'une demande d'entraide en l'absence d'un traité), et l'article 28, paragraphes 2 à 4 (relatifs à la confidentialité de la réponse et à l'imposition de conditions restrictives en l'absence d'un traité), de la Convention s'appliquent à l'article sur la vidéoconférence.

Paragraphe 3

195. Étant donné que, pour une vidéoconférence, il se peut que des personnels judiciaires et auxiliaires de justice de la Partie requérante doivent être disponibles pour participer au recueil du témoignage ou de la déposition dans la Partie requise, qui peut se trouver à plusieurs fuseaux horaires de distance de la Partie requérante, il faut absolument que la personne auditionnée soit sur place à l'heure dite. En vertu du paragraphe 3, lorsque la Partie requise prête son concours au titre du présent article, elle doit faire tout son possible pour obtenir la comparution de la personne dont le témoignage ou la déposition est requis. Les solutions les plus appropriées peuvent être tributaires des circonstances de l'affaire, ou du cadre du droit interne de la Partie requise ; la question peut également se poser du degré de confiance à accorder à la comparution volontaire de la personne au moment prévu. En revanche, pour garantir la comparution de la personne, il peut être souhaitable que la Partie requise délivre une injonction ou une citation à comparaître, et ce paragraphe l'y autorise, conformément aux garanties prévues par son droit interne.

Paragraphe 4

196. La procédure pour mener les vidéoconférences est exposée au paragraphe 4. L'objectif essentiel consiste à fournir le témoignage ou la déposition à la Partie requérante sous une forme qui lui permettra de s'en servir comme

preuve dans son enquête et sa procédure. C'est pourquoi ce sont les procédures demandées par la Partie requérante qui seront suivies, à moins qu'elles ne soient contraires aux dispositions légales de la Partie requise, notamment aux principes juridiques applicables dans la Partie requise qui ne sont pas codifiés dans sa législation. Ainsi, durant la vidéoconférence, il s'agirait de privilégier la procédure selon laquelle la Partie requise autorise les autorités de la Partie requérante à interroger directement la personne dont on veut obtenir le témoignage ou la déposition. Cette tâche incombera au procureur, juge d'instruction ou enquêteur de la Partie requérante, qui connaît le mieux l'enquête pénale ou les poursuites et est donc le mieux placé pour savoir quelles sont les questions à poser qui seront les plus utiles à l'enquête ou aux poursuites ainsi que la meilleure manière de les poser pour se conformer au droit de la Partie requérante. Dans ce cas, l'autorité de la Partie requise participant à l'audition n'interviendra que si cela est nécessaire du fait que l'autorité de la Partie requérante a eu un comportement incompatible avec le droit de la Partie requise. Elle pourra alors réfuter des questions, reprendre elle-même l'interrogatoire ou procéder à tout acte approprié en vertu de son droit et des circonstances dans lesquelles se déroule la vidéoconférence. L'expression « incompatible avec le droit de la Partie requise » ne couvre pas des situations dans lesquelles la procédure est simplement différente de celle qui a cours dans la Partie requise, ce qui sera souvent le cas. Elle vise plutôt des situations dans lesquelles la procédure est contraire au droit de la Partie requise ou ne peut pas fonctionner dans ce cadre. En un tel cas, ou si la Partie requérante n'a pas demandé de procédure spécifique, la procédure par défaut sera celle qui s'applique dans le droit interne de la Partie requise. Si l'application du droit de la Partie requise pose un problème à la Partie requérante, par exemple pour ce qui est de l'admissibilité du témoignage ou de la déposition lors du procès, les Parties requérante et requise peuvent chercher à s'entendre sur une procédure différente qui satisfera la Partie requérante tout en évitant le problème potentiel dans le droit de la Partie requise.

Paragraphe 5

197. Le paragraphe 5, qui concerne la peine ou sanction applicable pour faux témoignage, refus de répondre et autres comportements répréhensibles, a pour but de protéger l'intégrité du processus de recueil d'un témoignage ou d'une déposition lorsque le témoin se trouve physiquement dans un autre pays que celui où se déroule la procédure pénale. Dans la mesure où la Partie requise a fait obligation à la personne entendue de témoigner, de dire toute la vérité, ou qu'elle lui a interdit certains comportements (notamment le fait de perturber la

procédure), la personne entendue subira la conséquence de ses actes prévue dans la juridiction où elle se trouve. En de tels cas, la Partie requise doit pouvoir appliquer la sanction qu'elle appliquerait si le comportement répréhensible s'était produit dans le cadre de l'une de ses procédures nationales. La sanction s'applique sans préjudice d'une éventuelle compétence de la Partie requérante. Cette condition est une incitation supplémentaire pour que le témoin témoigne, témoigne sincèrement et ne se livre pas à un comportement répréhensible. Si aucune sanction n'est prévue dans les procédures en droit interne de la Partie requise (par exemple pour faux témoignage par une personne inculpée), il n'est pas demandé d'en prévoir une pour un tel comportement commis durant une vidéoconférence. Cette disposition sera particulièrement utile pour permettre de poursuivre un témoin faisant un faux témoignage mais qui ne peut être extradé pour être poursuivi dans la Partie requérante du fait par exemple que la Partie requise interdit l'extradition de ses ressortissants.

Paragraphe 6

198. Le paragraphe 6 prévoit des règles concernant la couverture des frais liés à des vidéoconférences. De manière générale, les frais engendrés dans le cadre d'une vidéoconférence sont supportés par la Partie requise, sauf pour ce qui concerne: 1. les honoraires d'un témoin expert ; 2. les frais de traduction, d'interprétation et de transcription ; et 3. des coûts si élevés qu'ils en deviennent exceptionnels. Les frais de voyage et d'hébergement dans la Partie requise sont la plupart du temps négligeables et en général couverts par cette dernière, si tel est le cas. Les règles en matière de couverture des coûts peuvent cependant être modifiées d'un commun accord entre les Parties requérante et requise. Ainsi, si la Partie requérante prévoit que la présence d'un interprète sera nécessaire ou qu'il lui faudra des services de transcription de la vidéoconférence, il est possible que la Partie requise ne paie pas pour la prestation de ces services. Quand la Partie requise prévoit des frais exceptionnels pour la fourniture de l'entraide, conformément au paragraphe 6.b, la Partie requérante et la Partie requise se concertent préalablement à l'exécution de la demande pour déterminer si la Partie requérante peut supporter ces frais et, dans le cas contraire, comment les éviter.

Paragraphe 7

199. Si le paragraphe 1 autorise expressément l'utilisation de la technologie de vidéoconférence pour le recueil d'un témoignage ou d'une déposition, le paragraphe 7.a prévoit que les dispositions de l'article 11 peuvent, sur consentement mutuel, être appliquées aux fins de la réalisation d'une audio-conférence.

De plus, le paragraphe 7.b prévoit que, sur consentement mutuel des Parties requérante et requise, la technologie peut être utilisée à d'autres « fins, pour des auditions [...] par exemple l'identification de personnes ou d'objets ». Ainsi, si elles en sont convenues, les Parties requérante et requise peuvent envisager d'utiliser la technologie de vidéoconférence pour auditionner ou mener des procédures concernant un suspect ou un inculpé (on relèvera que certaines Parties peuvent considérer qu'un suspect ou un inculpé est un « témoin », de sorte que le recueil de son témoignage ou de sa déposition serait déjà couvert par les dispositions du paragraphe 1 du présent article). Si le paragraphe 1 n'est pas applicable, il est possible de s'appuyer juridiquement sur le paragraphe 7 pour autoriser l'utilisation de cette technologie dans ces cas-là.

Paragraphe 8

200. Le paragraphe 8 traite la situation dans laquelle la Partie requise choisit d'autoriser l'audition d'un suspect ou inculpé par exemple pour recueillir un témoignage ou une déposition ou des déclarations, ou aux fins de notifications ou pour d'autres mesures procédurales. Tout comme la Partie requise a toute latitude pour autoriser l'utilisation de la vidéoconférence en vue d'entendre un témoin ordinaire ou expert, elle peut en faire de même pour ce qui est d'entendre un suspect ou un inculpé. De plus, outre toute autre condition ou limitation qu'une Partie requise peut imposer pour autoriser la tenue d'une vidéoconférence, le droit interne d'une Partie peut prévoir des conditions particulières concernant l'audition de suspects ou d'inculpés. Par exemple, exiger le consentement du suspect ou de l'accusé pour fournir un témoignage ou une déclaration, ou la loi d'une Partie peut interdire ou limiter l'utilisation de la vidéoconférence pour les notifications ou autres mesures procédurales. Le paragraphe 8 est donc conçu pour insister sur le fait que les procédures visant un suspect ou un inculpé peuvent entraîner la nécessité de mettre en place des conditions ou garanties en complément de celles qui s'appliqueraient par ailleurs.

Article 12 – Équipes communes d'enquête et enquêtes communes

201. La cybercriminalité et la preuve électronique étant par nature transnationales, les enquêtes et poursuites qui y sont relatives présentent souvent des liens avec d'autres États. Les équipes communes d'enquête (ECE) peuvent être un moyen efficace de coopération ou coordination opérationnelles entre deux États ou plus. L'article 12 donne une base pour de telles formes de coopération.

202. L'expérience a montré que, lorsqu'un État enquête sur une infraction ayant une dimension transfrontalière en lien avec la cybercriminalité ou pour laquelle il faut obtenir des preuves électroniques, l'enquête peut tirer parti de la participation des autorités d'autres États qui sont également en train d'enquêter sur les mêmes actes ou des actes connexes, ou bénéficier utilement d'une coordination.

203. Comme cela est indiqué à l'article 5 du présent Protocole et aux paragraphes 182 à 186 du présent rapport explicatif, les dispositions de l'article 12 ne s'appliquent pas en présence d'un traité d'entraide judiciaire ou d'un arrangement sur la base de dispositions législatives uniformes ou réciproques en vigueur entre les Parties requérante et requise, à moins que les Parties concernées ne conviennent d'appliquer tout ou partie du reste de cet article en leur lieu et place, si le traité ou l'arrangement ne l'interdit pas. Comme cela est expliqué ci-dessous, le paragraphe 7 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les parties concernées.

Paragraphe 1

204. Le paragraphe 1 prévoit que les autorités compétentes de deux Parties ou plus peuvent convenir d'établir une ECE lorsqu'elles l'estiment particulièrement utile. La participation à une ECE se fait par accord mutuel. Les termes « commun accord », « accord » et « convenir » – tels qu'utilisés à l'article 12 – ne devraient pas être compris comme comprenant la nécessité d'un accord contraignant au sens du droit international.

205. Le présent article utilise deux expressions liées: « autorités compétentes » et « autorités participantes ». Chaque Partie détermine quelles sont les autorités compétentes – les « autorités compétentes » – pour conclure un accord établissant une ECE. Certaines Parties peuvent y autoriser un ensemble de fonctionnaires tels que des procureurs, des juges d'instruction ou également des officiers de police de haut rang dirigeant des enquêtes ou procédures pénales à participer à ce type d'accord ; d'autres peuvent autoriser l'autorité centrale – le service normalement responsable des questions d'entraide – à le faire. De même, la détermination des autorités qui participent effectivement à une ECE – les « autorités participantes » – relève respectivement des Parties concernées.

Paragraphe 2

206. Le paragraphe 2 prévoit que les procédures et modalités régissant le fonctionnement des équipes communes d'enquête, telles que leurs objectifs spécifiques, leur composition ; leurs fonctions ; leur durée et toute éventuelle

prolongation ; leur emplacement ; leur organisation ; les conditions de recueil, de transmission et d'utilisation des informations ou preuves ; les conditions de confidentialité ; et les conditions de l'implication des autorités participantes d'une Partie dans des mesures d'enquête se déroulant sur le territoire d'une autre Partie, feront l'objet d'un accord entre les autorités compétentes concernées. En particulier, lorsqu'elles préparent le contenu de l'accord, les Parties concernées peuvent souhaiter établir des critères de refus ou de restriction de l'utilisation des informations et preuves y compris, par exemple, pour les motifs établis aux paragraphes 4 ou 5 de l'article 27 de la Convention, et préciser la procédure à suivre si ces dernières sont nécessaires pour des finalités autres que celles qui avaient présidé à l'établissement de l'accord (y inclus l'utilisation des informations ou preuves par le ministère public ou la défense dans une autre affaire ou leur utilisation pour prévenir une situation d'urgence telle que définie à l'article 3, paragraphe 2.c, c'est-à-dire présentant un risque significatif et imminent pour la vie ou la sécurité d'une personne physique). Les Parties sont encouragées à spécifier dans l'accord les limites des pouvoirs des personnes habilitées participantes d'une Partie qui sont physiquement présentes sur le territoire d'une autre Partie. Les Parties sont également encouragées à permettre dans l'accord la transmission électronique des informations ou preuves recueillies.

207. Il est supposé que les Parties établissent généralement par écrit ces procédures et conditions. Dans tout accord, il conviendrait de tenir compte du niveau de détail requis. Un texte simplifié peut présenter le niveau de précision nécessaire pour des situations prévisibles, avec la possibilité d'ajouter des dispositions supplémentaires si les circonstances exigeaient davantage de précisions. Les Parties prendront en compte le champ d'application territorial et la durée de l'accord établissant l'ECE, et le fait que l'accord pourrait nécessiter d'être modifié ou étendu en cas de faits nouveaux.

208. Les informations ou preuves utilisées dans le cadre de l'équipe commune d'enquête peuvent inclure des données à caractère personnel sous la forme de données relatives aux abonnés, de données de trafic ou de données de contenu. Comme pour d'autres mesures de coopération couvertes par le Protocole, l'article 14 s'applique au transfert de données à caractère personnel dans le cadre d'ECE.

209. Comme c'est généralement le cas pour toutes informations ou preuves reçues par une Partie en vertu du Protocole, les règles de la preuve applicables dans le droit interne de la Partie régiront l'admissibilité des informations ou preuves dans les procédures judiciaires.

Paragraphe 3

210. Le paragraphe 3 permet à une Partie de déclarer, au moment de sa signature ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, que son autorité centrale doit être signataire de l'accord portant création de l'équipe ou y souscrire d'une autre manière. Cette disposition a été insérée pour plusieurs raisons. Tout d'abord, plusieurs Parties considèrent que les ECE constituent une forme d'entraide. De plus, dans plusieurs autres Parties, les autorités centrales chargées de l'entraide peuvent avoir un rôle à jouer pour garantir que les conditions de droit interne applicables sont remplies lorsque les autorités compétentes (qui peuvent être des procureurs ou des services de police à l'expérience relativement limitée en matière de coopération internationale) préparent un accord établissant une ECE en vertu de cet article. L'expérience d'une autorité centrale en matière d'accords internationaux régissant l'entraide et d'autres formes de coopération internationale (y compris aux termes du présent Protocole) peut aussi l'aider à jouer un rôle précieux pour garantir le respect des conditions fixées par le Protocole. Enfin, lorsqu'une Partie a fait une déclaration en vertu de ce paragraphe, les autorités des autres Parties souhaitant établir une ECE avec la partie déclarante savent que l'autorité centrale de la Partie déclarante doit signer l'accord établissant l'ECE ou y souscrire d'une autre manière afin que cet accord soit valide en vertu du Protocole. Cette disposition empêche la conclusion d'un accord établissant une ECE qui n'aurait pas reçu l'autorisation requise ou qui ne serait pas conforme aux conditions légales applicables de la Partie déclarante.

Paragraphe 4

211. En vertu du paragraphe 4, les autorités compétentes déterminées par les Parties en vertu du paragraphe 1 et les autorités participantes visées au paragraphe 2 communiqueront en principe directement entre elles dans un souci d'efficacité et d'efficacité. Cependant, si des circonstances exceptionnelles exigent une coordination plus centrale – par exemple dans des affaires présentant des ramifications particulièrement graves ou des situations présentant des problèmes particuliers de coordination –, il peut être convenu d'autres canaux appropriés. Ainsi, les autorités centrales chargées de l'entraide peuvent être sollicitées pour aider à se coordonner dans ces circonstances.

Paragraphe 5

212. Le paragraphe 5 prévoit que, si des mesures d'enquêtes doivent être prises sur le territoire de l'une des Parties participantes, les autorités participantes de

cette dernière peuvent demander à leurs propres autorités d'effectuer lesdites mesures. Ces dernières déterminent en fonction de leur droit interne si elles le peuvent. Si elles sont en mesure de le faire, il n'est pas nécessaire que d'autres Parties participantes présentent une demande d'entraide. Cette disposition couvre l'un des aspects les plus innovants des ECE. Toutefois, dans certains cas, il est possible que ces autorités n'aient pas la compétence nécessaire en droit interne pour effectuer une mesure d'enquête pour le compte d'une autre Partie sans demande d'entraide.

Paragraphe 6

213. Le paragraphe 6 traite de l'utilisation des informations ou preuves communiquées aux autorités participantes d'une Partie par les autorités participantes d'une autre Partie. L'utilisation peut être refusée ou limitée conformément aux termes d'un accord tel que visé aux paragraphes 1 et 2 ; toutefois, si cet accord ne prévoit rien en termes de refus ou de limitation de l'utilisation, les informations ou preuves peuvent être utilisées selon les modalités prévues au paragraphe 6.a à c. Les circonstances prévues au paragraphe 6 s'appliquent sans préjudice des conditions fixées pour les transferts ultérieurs d'informations ou de preuves à un autre État telles que prévues à l'article 14.

214. Il convient de noter que, lorsque les paragraphes 6.a à c s'appliquent, les autorités participantes peuvent néanmoins convenir entre elles de limiter davantage l'utilisation d'informations ou preuves particulières pour éviter de nuire à l'une de leurs enquêtes, soit avant, soit après la fourniture des informations ou preuves. Ainsi, même si l'utilisation de preuves par la Partie qui les a reçues répond à l'un des objectifs pour lesquels l'ECE avait été établie, cela peut nuire à l'enquête de la Partie qui fournit les informations ou preuves (par exemple en révélant à un groupe criminel qu'une enquête est en train d'être menée sur eux, ce qui risque de les faire fuir, de les amener à détruire des preuves ou à intimider des témoins). Dans ce cas, la Partie qui a fourni les informations ou preuves peut demander à l'autre Partie d'accepter de ne pas les rendre publiques tant que le risque n'a pas disparu.

215. Au paragraphe 6.b, les rédacteurs visaient la situation où, en l'absence d'accord prévoyant les conditions du refus ou de la limitation de l'utilisation, il ne serait pas nécessaire d'obtenir le consentement des autorités les ayant fournies dans le cas où, en vertu des principes juridiques fondamentaux de la Partie dont les autorités participantes les ont reçues, ces informations ou

preuves importantes pour une défense effective dans une procédure concernant d'autres infractions doivent être absolument divulguées à la défense ou à une autorité judiciaire. Même si, dans ce cas, le consentement n'est pas exigé, la divulgation des informations et preuves à cette fin sera notifiée sans retard indu. Si possible, la notification devrait intervenir avant la divulgation, afin de permettre à la Partie qui a fourni les informations ou preuves de se préparer à leur divulgation et de mettre les Parties en mesure de se consulter en tant que de besoin.

216. Selon la compréhension des rédacteurs, le paragraphe 6.c fait référence à des circonstances exceptionnelles dans lesquelles les autorités de la Partie destinataire pourraient utiliser directement les informations ou preuves pour prévenir une urgence, telle que définie à l'article 3, paragraphe 2.c, de ce Protocole. La sécurité d'une personne physique signifie des dommages corporels graves. La notion de « risque significatif et imminent pour la vie ou la sécurité d'une personne » est expliquée plus en détail dans le présent rapport explicatif, au paragraphe 42, qui fournit aussi des exemples de ce type de situation. Les rédacteurs ont considéré que cette notion incluait les situations dans lesquelles un risque significatif et imminent pour des biens ou réseaux met en cause la vie ou la sécurité d'une personne physique. Si des informations ou preuves sont utilisées en application du paragraphe 6.c, les autorités participantes de la Partie qui les a fournies doivent en être notifiées sans retard indu sauf autre accord. Ainsi, par exemple, les autorités participantes peuvent décider que l'autorité centrale devrait être notifiée.

Paragraphe 7

217. Enfin, il convient de rappeler de manière générale qu'il existe une longue histoire de coopération internationale mise en œuvre directement au cas par cas entre partenaires des services répressifs, dans le cadre de laquelle une équipe de procureurs et/ou d'enquêteurs d'un pays coopère avec ses homologues étrangers dans une enquête spécifique, selon un format autre que celui d'une ECE. Le paragraphe 7 couvre ces cas de coopération internationale et, pour les Parties qui en auraient besoin, fournit une base juridique pour mener une enquête conjointe sans un accord tel que visé aux paragraphes 1 et 2. Ce paragraphe s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base d'une législation uniforme et réciproque en vigueur entre les Parties concernées. Comme pour toutes les mesures prévues par le présent protocole, les enquêtes conjointes visées au paragraphe 7 sont soumises aux conditions et garanties du chapitre III.

Chapitre III – Conditions et garanties

Article 13 – Conditions et garanties

218. Fondé sur l'article 15 de la Convention, l'article 13 du Protocole prévoit que « 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 ». Cet article étant fondé sur l'article 15 de la Convention, l'explication de cet article aux paragraphes 145 à 148 du rapport explicatif de la Convention est également valable pour l'article 13 du présent Protocole, notamment le fait que le principe de proportionnalité « est mis en œuvre par chaque Partie conformément aux principes pertinents de son droit interne » (voir paragraphe 146 du rapport explicatif de la Convention).

219. Il convient de noter qu'en plus de cet article d'autres articles contiennent des garanties importantes. Par exemple, les mesures prévues par le présent Protocole ont un champ d'application limité, c'est-à-dire « aux enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des systèmes et des données informatiques, et à la collecte de preuves sous forme électronique d'une infraction pénale » (voir article 2). En outre, certains articles précisent les informations à inclure dans les demandes, les ordonnances et les informations d'accompagnement qui peuvent aider à appliquer les garanties nationales (voir l'article 6, paragraphe 3 l'article 7, paragraphes 3 et 4 ; l'article 8, paragraphe 3 ; et l'article 9, paragraphe 3). En outre, les types de données à divulguer sont précisés dans chaque article, comme à l'article 7 qui est limité aux informations sur les abonnés. De plus, les Parties peuvent émettre des réserves et des déclarations, par exemple pour limiter le type d'informations à fournir comme dans les articles 7 et 8. Enfin, lorsque des données à caractère personnel sont transférées en vertu du présent Protocole, les garanties de protection des données de l'article 14 s'appliquent.

Article 14 – Protection des données à caractère personnel

Paragraphe 1 – Champ d'application

220. Les mesures prévues au chapitre II du présent Protocole nécessitent souvent le transfert de données à caractère personnel. Étant donné qu'un grand nombre de Parties au Protocole peuvent être tenues, pour se conformer à leurs obligations constitutionnelles ou internationales, d'assurer la protection des données à caractère personnel, l'article 14 prévoit des garanties de

protection des données à caractère personnel pour permettre aux Parties de satisfaire à ces obligations et de rendre ainsi possible le traitement de données à caractère personnel aux fins du présent Protocole.

221. En vertu du paragraphe 1.a, chaque Partie est tenue de traiter les données à caractère personnels qu'elle reçoit en vertu du présent Protocole conformément aux garanties expressément prévues aux paragraphes 2 à 15. Sont également couvertes les données à caractère personnel transférées en exécution d'une injonction ou d'une demande faite en vertu du présent Protocole. Toutefois, les paragraphes 2 à 15 ne s'appliquent pas si les conditions des exceptions exposées aux paragraphes 1.b ou 1.c sont applicables.

222. La première exception figure au paragraphe 1.b, qui dispose que « [s] i, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie transférante et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, 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, sauf accord contraire entre les Parties concernées. » À cet égard, un cadre serait généralement considéré comme « global » s'il couvre l'ensemble des aspects de la protection des données pour les transferts de données. Deux exemples d'accords visés au paragraphe 1.b sont 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 STCE n° 223 et l'Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Les termes de ces accords s'appliquent en lieu et place des paragraphes 2 à 15 en ce qui concerne les mesures entrant dans leur champ d'application. À l'égard des Parties à la Convention STE n° 108 telle qu'amendée par le Protocole STCE n° 223, il en résulte que l'article 14, paragraphe 1 de ce traité, tel qu'expliqué en détail aux paragraphes 105 à 107 de son rapport explicatif, est applicable. En termes de chronologie, les paragraphes 2 à 15 de cet article ne seront subrogés que si les Parties sont mutuellement liées par l'accord au moment de

la réception de données à caractère personnel en vertu du présent Protocole. Cela vaut aussi longtemps que l'accord dispose que les données à caractère personnel transférées en application de ses dispositions continueront d'être traitées dans les conditions qu'il définit.

223. La seconde exception est exposée au paragraphe 1.c, qui dispose que, même si la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord du type de celui décrit au paragraphe 1.b, elles peuvent néanmoins déterminer conjointement que le transfert de données à caractère personnel en vertu du présent Protocole peut se faire sur la base d'autres accords ou arrangements en lieu et place des paragraphes 2 à 15 de cet article. Cela garantit aux Parties une certaine souplesse pour fixer les garanties de protection des données qui s'appliquent aux transferts effectués entre elles en vertu du présent Protocole. Dans un souci de sécurité juridique et de transparence pour les individus et pour les fournisseurs et les entités impliqués dans les transferts de données en application des mesures prévues à la section 2 du chapitre II de ce Protocole, les Parties sont encouragées à communiquer clairement au public leur détermination commune à ce qu'un accord ou un arrangement de cette nature régit les aspects relatifs à la protection des données lors des transferts de données à caractère personnel entre elles.

224. Les rédacteurs ont considéré que le Protocole garantissait des protections satisfaisantes pour les transferts de données effectués en application de ses dispositions grâce aux garanties de protection des données prévues aux paragraphes 2 à 15. À cette fin, conformément au paragraphe 1.d, les transferts de données visés au paragraphe 1.a seront réputés satisfaire aux exigences du cadre juridique de chacune des Parties régissant la protection des données pour les transferts internationaux de données à caractère personnel ; en conséquence, aucune autre autorisation ne sera requise en vertu de ces cadres juridiques pour ces transferts. En outre, dans la mesure où les dispositions des accords décrits au paragraphe 1.b établissent que le traitement des données à caractère personnel en vertu de ces accords satisfait aux exigences de la législation des Parties concernées relative à la protection des données, le paragraphe 1.d étend cette approbation aux transferts effectués en vertu du présent Protocole. Ce paragraphe 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. Comme les accords ou

arrangements décrits au paragraphe 1.c ne font pas nécessairement mention de la conformité au cadre juridique des Parties relatif à la protection des données lors de transferts internationaux – par exemple dans le cas des traités bilatéraux d'entraide judiciaire –, ils ne reçoivent pas la même approbation en vertu de ce Protocole que dans les cas relevant des paragraphes 1.a ou 1.b. Toutefois, les Parties concernées peuvent décider d'un commun accord que cette approbation est acquise.

225. De plus, 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 lorsque le paragraphe 1.a 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.

226. Enfin, l'objectif de l'article 14 est d'établir des garanties satisfaisantes pour permettre le transfert de données à caractère personnel entre les Parties au présent Protocole. L'article 14 n'impose pas une harmonisation des cadres juridiques nationaux régissant le traitement général des données à caractère personnel ni du cadre relatif au traitement spécifique des données à caractère personnel aux fins de l'application du droit pénal. Le paragraphe 1.e dispose que rien n'empêche les Parties d'appliquer des garanties plus strictes que celles prévues aux paragraphes 2 à 15 pour le traitement, par leurs autorités respectives, des données à caractère personnel reçues en vertu du présent Protocole. Inversement, le paragraphe 1.e n'a pas pour but de permettre aux Parties d'imposer des conditions supplémentaires de protection des données autres que celles expressément prévues dans cet article pour les transferts de données effectués en vertu du présent Protocole.

Paragraphe 2 – But et utilisation

227. Le paragraphe 2 traite des buts et de l'utilisation pour lesquels les Parties peuvent procéder au traitement de données à caractère personnel en vertu du présent Protocole. Le paragraphe 2.a dispose que « la Partie destinataire de données personnelles (« Partie destinataire ») traite les données aux fins prévues à l'article 2 », c'est-à-dire aux fins « [d']enquêtes ou [de] procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques » et de « recueil de preuves d'une infraction pénale sous forme électronique », et, pour ce qui concerne les Parties au Premier Protocole, aux fins « d'enquêtes ou procédures pénales spécifiques concernant

les infractions pénales établies dans le Premier Protocole ». En d'autres termes, 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 de rechercher des preuves ou des informations contenant des données à caractère personnel et de les traiter.

228. Si la raison première pour laquelle le Protocole peut être invoqué est uniquement l'obtention d'informations ou de preuves dans une enquête ou une procédure pénale donnée, à l'exclusion d'autres fins, le paragraphe 2.a dispose aussi qu'une Partie « ne [doit pas procéder] à d'autres traitements des données personnelles à des fins incompatibles et [qu']elle ne traite pas non plus les données lorsque son cadre juridique ne l'autorise pas ». Pour déterminer si la finalité d'un traitement supplémentaire n'est pas incompatible avec le but initial, l'autorité compétente est encouragée à procéder à une évaluation globale des circonstances de l'espèce comme (i) le rapport entre le but initial et le but supplémentaire ultérieur (établi par un éventuel lien objectif, par exemple) ; (ii) les conséquences (potentielles) pour les personnes concernées de l'utilisation supplémentaire envisagée, en tenant compte de la nature des données à caractère personnel (leur sensibilité, par exemple) ; (iii) les attentes raisonnables potentielles des personnes concernées quant au but de cette utilisation supplémentaire et à l'égard des entités qui pourraient traiter les données, et iv. la manière dont les données seront traitées et protégées contre toute utilisation indue. Le cadre juridique d'une Partie peut fixer des limites particulières concernant d'autres objectifs pour lesquels les données peuvent être utilisées.

229. Le traitement des données dans un but qui ne soit pas incompatible devrait normalement comprendre leur utilisation à des fins de coopération internationale conformément aux législations nationales et aux accords ou arrangements internationaux en matière pénale (pour l'entraide judiciaire, par exemple). Il pourrait aussi inclure, entre autres, des utilisations dans le cadre de certaines fonctions administratives, comme les déclarations aux organes de contrôle, les enquêtes connexes sur des infractions au droit pénal, civil ou administratif (y compris les enquêtes menées par d'autres instances administratives) et leur jugement, les divulgations ordonnées par décision de justice, la divulgation à des personnes privées parties à un litige, la communication de certaines informations à l'avocat d'un accusé et la divulgation directe au public ou aux médias (y compris dans le cadre des demandes d'accès aux documents et de procédures judiciaires publiques). De même, un traitement

supplémentaire des données à caractère personnel à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique, ou à des fins statistiques pourrait être considéré comme compatible.

230. Le paragraphe 2.a autorise en outre les Parties à imposer des conditions et restrictions supplémentaires à l'utilisation de données à caractère personnel dans des cas donnés, dans la mesure prévue au chapitre II du présent Protocole. Toutefois, ces conditions ne doivent pas comporter de conditions génériques de protection des données – c'est-à-dire des conditions qui ne soient pas propres à des cas donnés – allant au-delà de celles prévues par le paragraphe 14. À titre d'exemple, différents systèmes de supervision sont admis en vertu de l'article 14 et une Partie n'est pas autorisée à poser comme condition préalable au transfert de données dans un cas individuel que la Partie requérante dispose de l'équivalent d'une autorité spécialisée de protection des données.

231. Enfin, le paragraphe 2.b fait obligation à la Partie destinataire, lorsqu'elle cherche à obtenir des données à caractère personnel et les utilise en vertu du présent Protocole, « [de veiller], dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement ». Cette obligation peut par exemple être mise en œuvre au moyen des règles de la preuve et de limitations de la portée des injonctions contraignantes, des principes de nécessité, de proportionnalité et du caractère raisonnable, et de directives et politiques internes limitant la collecte ou l'utilisation des données. Les Parties sont également encouragées à considérer, dans leurs cadres juridiques nationaux, les situations impliquant des personnes vulnérables, comme les victimes ou les mineurs, par exemple.

Paragraphe 3 – Qualité et intégrité

232. Le paragraphe 3 impose aux Parties de prendre « des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte et complète, et soient aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi compte tenu des buts dans lesquels elles sont traitées ». Le contexte est important et ce principe peut donc être mis en œuvre différemment selon les situations. Il ne s'appliquerait par exemple pas de la même manière à des fins de poursuites pénales que dans d'autres buts.

233. S'agissant des enquêtes et des procédures pénales, le paragraphe 3 ne doit pas être interprété dans le sens qu'il imposerait aux autorités de poursuites

pénales de modifier les informations qui pourraient servir de preuves dans une affaire pénale – même lorsque ces informations sont inexactes ou incomplètes –, parce que l'inexactitude de ces données peut être un élément majeur de l'infraction (par exemple en cas de fraude) et parce que cela saperait en outre l'objectif d'équité à l'égard de l'accusé si les autorités modifiaient une preuve recueillie grâce au présent Protocole.

234. Dans de nombreuses situations, lorsqu'il y a des doutes quant à la fiabilité des données à caractère personnel, cela devrait être clairement indiqué. Par exemple, dans la mesure où des informations ou des preuves qui ont été reçues grâce au présent Protocole sont utilisées pour retracer une conduite criminelle passée, les procédures applicables devraient prévoir les moyens de corriger ou de garder la trace des erreurs dans les informations (notamment en modifiant ou en complétant les informations originales) et d'actualiser, modifier ou compléter les données peu fiables ou obsolètes afin de minimiser le risque que les autorités prennent des mesures répressives inappropriées ou potentiellement défavorables sur la base de données de mauvaise qualité (par exemple en arrêtant la mauvaise personne ou en arrêtant une personne en s'appuyant sur une compréhension erronée de son comportement). Les Parties sont encouragées à prendre des mesures raisonnables pour s'assurer que, lorsque des données communiquées à une autre autorité ou reçues d'une autre autorité se révèlent inexactes ou obsolètes, cette autre autorité en est informée aussi rapidement que possible afin qu'il puisse être procédé aux corrections nécessaires et appropriées compte tenu des finalités du traitement.

Paragraphe 4 – Données sensibles

235. Le paragraphe 4 concerne les mesures qui doivent être prises par les Parties en vertu du présent Protocole lorsqu'elles traitent certains types de données qui peuvent être nécessaires, en particulier, à titre de preuves dans une enquête ou une procédure pénale mais dont la nature impose que des garanties appropriées soient prises pour se prémunir contre le risque d'effets préjudiciables injustifiés pour la personne concernée par l'utilisation de ces données, en particulier contre le risque de discrimination illicite.

236. Aux termes du paragraphe 4, les données sensibles sont notamment « les données à caractère personnel révélant l'origine ethnique ou raciale ; les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale ; ainsi que [les] données génétiques, [les] données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent ; ou [les] données à caractère personnel concernant la santé ou la sexualité »,

ce dernier élément recouvrant à la fois l'orientation sexuelle et les pratiques sexuelles. Les données relatives à la santé peuvent comprendre des données relatives à la santé physique ou mentale d'une personne qui révèlent des informations sur son état de santé passé, présent ou futur (comme des informations sur une maladie, un handicap, un risque de maladie, l'historique médical d'une personne ou ses traitements, ou encore son état physiologique ou biomédical). Les données génétiques peuvent comprendre, par exemple, les résultats d'analyses chromosomiques, d'ADN ou d'ARN qui concernent les caractéristiques génétiques héritées ou acquises d'une personne et contiennent des informations uniques sur sa physiologie, sa santé ou sa filiation.

237. La notion de données biométriques couvre toute une série d'identifiants uniques résultant de caractéristiques physiques ou physiologiques mesurables utilisées pour identifier une personne ou vérifier l'identité déclarée par cette dernière (empreintes digitales, motif de l'iris ou des veines de la main, schémas vocaux, photographies ou séquences vidéo, par exemple). Certaines Parties considèrent aussi que les identifiants uniques fournis par des caractéristiques biologiques ou comportementales constituent des données biométriques. 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. Ainsi, certaines Parties considèrent que les données biométriques qui sont informatisées ou extraites d'un échantillon ou d'une image biométrique (comme les modèles biométriques) sont des données sensibles. Inversement, certaines photographies ou séquences vidéo, même si elles révèlent des caractéristiques physiques ou anatomiques telles que des cicatrices, des marques sur la peau et des tatouages, ne seront généralement pas considérées comme des données biométriques sensibles. Puisque le niveau de sensibilité des données biométriques peut varier, le paragraphe 4 offre aux Parties une latitude pour régler cette question en indiquant que les données sensibles comprennent les « données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent ». Cette formulation reconnaît que la biométrie est un domaine en évolution et que les données considérées comme « sensibles » aux termes de ce paragraphe devront faire l'objet d'une évaluation dans la durée au regard des nouveautés technologiques et en matière de techniques d'enquête et autres, et compte tenu des risques qu'elles entraînent pour les personnes concernées. 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 No108) telle qu'amendée par le Protocole STCE No. 223, l'interprétation de ce qui constitue des données biométriques « sensibles » devrait être guidée

par l'article 6, paragraphe 1, de ce traité, tel que détaillé aux paragraphes 58 et 59 de son rapport explicatif.

238. L'utilisation abusive et le traitement indu de données sensibles présentent des risques de préjudice pour les personnes concernées, notamment des risques de discrimination illicite. Le système de justice pénale devrait être configuré de sorte à assurer une protection contre les conséquences préjudiciables injustifiées et la discrimination illicite fondée, par exemple, sur l'utilisation de preuves révélant la race, la religion ou la sexualité d'une personne. Pour donner un autre exemple, ce paragraphe reconnaît aussi l'importance de protéger contre le risque de préjudice causé par la divulgation injustifiée ou illégale afin d'éviter, par exemple, qu'une personne soit ostracisée en raison d'informations révélant son orientation sexuelle ou son identité de genre. À cet égard, le paragraphe 4 exige des Parties qu'elles mettent en place des « garanties appropriées » pour se prémunir contre ces risques.

239. Le caractère approprié des garanties devrait être apprécié au regard de la sensibilité des données, de la portée, du contexte, des buts et de la nature du traitement (par exemple en cas de prise de décisions automatisée) ainsi que de la probabilité et de la gravité des risques. Ces garanties peuvent varier d'un système juridique interne à l'autre et dépendre de ces facteurs. Une liste non exhaustive de garanties pourrait inclure la restriction du traitement des données (qui ne serait, par exemple, autorisé qu'au cas par cas ou à certaines fins), la limitation de leur diffusion, la restriction de l'accès à ces dernières (ouvert seulement à certains personnels, par exemple, en vertu de procédures spéciales d'autorisation ou d'authentification nécessitant une formation spécialisée de ces personnels), des mesures organisationnelles ou techniques de sécurité supplémentaires (comme le masquage, la pseudonymisation ou le stockage séparé des données biométriques et des informations biographiques correspondantes), ou des durées de conservation plus courtes. Dans certains cas, il peut être utile de procéder à une analyse d'impact pour faciliter l'identification et la gestion des risques.

Paragraphe 5 – Périodes de conservation

240. La première phrase du paragraphe 5 dispose que « [c]haque Partie conserve les données à caractère personnel uniquement pour la durée nécessaire et appropriée aux fins du traitement des données prévu au paragraphe 2 ». À cet égard, le principe de limitation des buts énoncé au paragraphe 2 dispose qu'une Partie destinataire de données à caractère personnel doit les traiter dans des buts définis conformément à l'article 2 et ne doit pas les soumettre à

d'autres traitements dans un but incompatible avec cet article. Conformément à ce principe, la durée de conservation des données dépend des buts définis dans lesquels ces données sont traitées.

241. En vertu de l'article 2, les données à caractère personnel reçues par une Partie en vertu du présent Protocole l'étant à des fins d'enquêtes ou de procédures pénales spécifiques, ces données peuvent être conservées aussi longtemps que nécessaire: a. pendant la durée de l'enquête et de la procédure subséquente, y compris les éventuelles procédures en appel ou la durée au cours de laquelle une affaire peut être rouverte en vertu du droit interne et b. pour faire l'objet d'un traitement supplémentaire dans un but qui n'est « pas incompatible » avec le but premier de la collecte après que celui-ci a été atteint. Ainsi, une Partie peut disposer que les informations ou preuves soient conservées à des fins d'archivage ou de recherches historiques, ou d'autres buts compatibles, conformément à l'article 14, paragraphe 2, comme exposé plus en détail dans les paragraphes correspondants du présent rapport explicatif.

242. La deuxième phrase du paragraphe 5 offre aux Parties deux possibilités pour satisfaire à l'obligation de ne pas conserver des données à caractère personnel plus longtemps que nécessaire et approprié au vu des finalités de leur traitement en vertu du paragraphe 2 de cet article. Premièrement, une Partie peut fixer des durées de conservation déterminées dans son droit interne. Sinon, les Parties peuvent prévoir dans leur droit interne que la nécessité de conserver plus longtemps les données soit revue à intervalles programmés. Les Parties disposent d'une marge discrétionnaire pour décider de l'approche la plus adaptée aux données concernées en l'espèce dans le contexte de leur cadre juridique interne. Les Parties peuvent aussi prévoir une durée de conservation déterminée assortie d'un système de révision périodique à intervalles plus courts. Elles devraient garantir dans leur cadre juridique que les autorités compétentes élaborent des règles et/ou procédures internes pour la mise en œuvre des durées de conservation déterminées et/ou des révisions périodiques de la nécessité de prolonger la conservation. Lorsque la durée de conservation est écoulée ou lorsque la Partie a établi, dans le cadre de la révision périodique, qu'il n'est plus nécessaire de conserver les données, celles-ci doivent être supprimées ou anonymisées.

Paragraphe 6 – Décisions automatisées

243. Le paragraphe 6 concerne la protection des personnes lorsque des décisions emportant des conséquences négatives importantes pour les intérêts en jeu pour elles sont fondées uniquement sur le traitement automatisé de

leurs données personnelles. Il ne devrait pas arriver fréquemment que des décisions soient prises de façon automatisée lorsqu'une Partie sera destinataire de données à caractère personnel provenant d'une autre Partie en vertu du présent Protocole car les preuves ou les informations seront recueillies par des enquêteurs ou des autorités judiciaires aux fins d'une enquête ou d'une procédure pénale déterminée. Néanmoins, lorsque la prise de décisions ayant un effet défavorable significatif sur les intérêts en jeu pour la personne à laquelle se rapportent les données à caractère personnel se fait de manière automatisée dans le cadre de l'enquête pour laquelle ces données ont été demandées, les autorités doivent appliquer cette disposition. Elles doivent aussi l'appliquer lorsque les données sont utilisées par la suite à des fins de prévention, de détection, d'enquête ou de poursuites relatives à d'autres infractions (arrestation fondée sur le traitement purement automatisé de profils criminels, de données relatives aux condamnations, aux libérations conditionnelles et sous caution, par exemple) ou dans un but compatible (par exemple dans le cadre de la vérification des antécédents), si les données font l'objet d'un traitement par des outils d'analyse automatisée pour la prise de décisions.

244. Par conséquent, le paragraphe 6 interdit les décisions fondées exclusivement sur le traitement automatisé de données à caractère personnel lorsque ces décisions ont des répercussions négatives importantes sur les intérêts en jeu pour la personne concernée, y compris sur le plan juridique (en raison des incidences sur la situation juridique ou les droits de l'intéressé), comme l'émission d'un mandat d'arrêt ou le refus d'une libération conditionnelle ou sous caution, à moins que cette prise de décisions automatisée soit autorisée en droit interne et s'accompagne de garanties appropriées.

245. Des garanties appropriées sont essentielles pour réduire l'impact potentiel sur les intérêts en jeu pour la personne à laquelle les données à caractère personnel se rapportent. Ces garanties devraient comprendre la possibilité pour la personne concernée d'obtenir une intervention humaine pour évaluer la décision. Les Parties sont également encouragées à prendre des mesures raisonnables pour assurer la qualité et la représentativité des données utilisées pour développer les algorithmes ainsi que l'exactitude des inférences statistiques utilisées en tenant compte des circonstances et du contexte spécifiques, y compris le contexte de l'application du droit pénal.

Paragraphe 7 – Sécurité des données et incidents de sécurité

246. En vertu du paragraphe 7.a, « [c]haque Partie s'assure de disposer de mesures technologiques, physiques et organisationnelles appropriées pour

la protection des données à caractère personnel ». Par exemple, ces mesures technologiques peuvent inclure des logiciels de protection contre les logiciels malveillants, le cryptage des données et des pare-feux. Les mesures physiques peuvent comprendre l'hébergement des serveurs et fichiers informatiques dans des lieux sécurisés et les mesures organisationnelles peuvent consister en diverses règles, pratiques, politiques et procédures, visant notamment à limiter les droits d'accès.

247. Le paragraphe 7.a dispose en outre que ces mesures doivent protéger en particulier contre la perte (par exemple au moyen de procédures standardisées pour l'enregistrement et le maniement des données), contre l'accès accidentel ou non autorisé (par exemple au moyen de protections contre les intrusions informatiques, de conditions d'autorisation ou d'authentification pour l'accès aux dossiers papier ou aux fichiers informatiques), contre la divulgation accidentelle ou non autorisée (par exemple au moyen de mesures technologiques de détection et de prévention des divulgations accidentelles ou non autorisées et de mesures organisationnelles pour indiquer les conséquences de telles divulgations) et contre l'altération ou la destruction accidentelle ou non autorisée de données (par exemple en restreignant la saisie ou la modification de données électroniques ou de dossiers papier au personnel autorisé, en utilisant des systèmes d'enregistrement, en affichant les durées de conservation ou en installant des systèmes de sauvegarde des fichiers informatiques et des dossiers papier).

248. Les modalités précises arrêtées pour satisfaire à ces obligations, d'une manière adaptée aux circonstances particulières de l'espèce, sont laissées à la discrétion de la Partie concernée. Les Parties sont par exemple encouragées à concevoir et à mettre en œuvre des mesures de sécurité qui prennent en compte des facteurs tels que la nature des données à caractère personnel (notamment leur sensibilité), les risques identifiés et les conséquences négatives potentielles pour la personne concernée en cas d'incident de sécurité. Les Parties peuvent aussi prendre en compte la question des ressources nécessaires pour la conception et l'application des mesures de sécurité des données. Elles sont encouragées à revoir périodiquement ces mesures et à les actualiser si nécessaire au vu de l'évolution de la technologie et de la nature des risques.

249. Le paragraphe 7.b expose les obligations en cas d'incident de sécurité (tel que défini au paragraphe 7.a et décrit ci-dessus) concernant les données à caractère personnel reçues en vertu du présent Protocole et créant un « risque significatif de préjudice matériel ou non matériel » aux personnes ou à la Partie de laquelle proviennent les données. Les préjudices aux personnes visés ici sont

notamment les préjudices corporels ou de réputation, la détresse émotionnelle (par exemple en raison de l'humiliation ou d'une violation de la confidentialité), la discrimination ou les préjudices financiers (par exemple en raison de la perte de l'emploi ou d'opportunités professionnelles, d'une note de la qualité de crédit négative, de l'usurpation d'identité ou du risque de chantage). Pour l'autre Partie, le risque peut en particulier résider dans l'impact négatif potentiel sur une enquête parallèle (par exemple avec la fuite du suspect ou la destruction de preuves). S'il y a un « risque significatif » que de tels préjudices surviennent, la Partie destinataire a l'obligation « [d'évaluer] sans tarder la probabilité de survenance et l'importance » du préjudice et de « prend[re] rapidement les mesures appropriées pour atténuer ce préjudice ». Les facteurs relatifs à la probabilité et à l'importance du préjudice à prendre en considération sont, entre autres, le type d'incident, comme le fait, s'il est connu, qu'il repose sur une intention de nuire et l'identité des personnes en possession des informations ou qui ont pu les obtenir, la nature et la sensibilité des données concernées, le volume de données potentiellement compromises et le nombre de personnes potentiellement touchées, la possibilité d'identifier facilement les personnes concernées, la probabilité qu'il y ait eu accès aux données et qu'elles aient été utilisées, selon qu'elles aient été cryptées, par exemple, ou rendues inaccessibles d'une autre manière, ainsi que les conséquences qui pourraient résulter de cet incident.

250. Conformément aux mesures décrites au paragraphe 7.a et afin d'apporter la réponse appropriée visée au paragraphe 7.b, les Parties sont tenues de disposer de procédures internes permettant de détecter les incidents de sécurité. Elles devraient également disposer d'une procédure leur permettant d'évaluer rapidement la probabilité de survenance d'un préjudice potentiel et son ampleur et de prendre rapidement les mesures appropriées pour le limiter (par exemple en demandant le retour ou la suppression des données transmises accidentellement à un destinataire non autorisé). L'application effective de ces obligations peut être facilitée par l'existence de procédures internes de signalement et par la consignation de tous les incidents de sécurité.

251. Le paragraphe 7.b énumère aussi les circonstances dans lesquelles l'autre Partie et les personnes concernées doivent recevoir notification de l'incident, sous réserve des exceptions et restrictions.

252. En cas d'incident de sécurité comportant un risque significatif de préjudice matériel ou non matériel à des personnes ou à l'autre Partie, notification doit en être faite à l'autorité transférante ou, aux fins de la section 2 du chapitre II, à l'autorité ou aux autorités désignées conformément au paragraphe 7.c. Toutefois, cette notification peut être assortie de restrictions appropriées

quant à la transmission de cette notification à des tiers ; elle peut être différée ou omise lorsqu'elle risque de porter atteinte à la sécurité nationale ou être différée lorsqu'elle risque de compromettre des mesures visant à protéger la sécurité publique (y compris lorsqu'elle compromettrait l'enquête sur les infractions pénales découlant de l'incident de sécurité). Pour décider s'il convient de différer ou d'omettre la notification dans des circonstances où celle-ci pourrait mettre en danger la sécurité nationale, une Partie devrait se demander s'il est raisonnable, dans ces circonstances, d'omettre la notification ou s'il ne serait pas plus approprié de la différer.

253. En cas d'incident de sécurité comportant un risque important de préjudice matériel ou non matériel à des personnes, les personnes concernées par cet incident doivent également en recevoir notification afin de pouvoir protéger leurs intérêts, cette obligation de notification étant toutefois soumise à des exceptions. Premièrement, le paragraphe 7.b indique qu'il n'est pas nécessaire de procéder à cette notification si la Partie a pris des mesures appropriées de sorte qu'il n'y a plus de risque significatif de préjudice. Par exemple, aucune notification ne serait nécessaire lorsqu'un e-mail contenant des informations personnelles sensibles a été envoyé par mégarde au mauvais destinataire, ce qui aurait constitué un risque significatif de préjudice sans mesures d'atténuation de ce risque, mais que le destinataire a, sur demande, rapidement et définitivement supprimé ce message sans qu'il soit diffusé plus largement. Deuxièmement, la notification à une personne peut être omise ou différée dans les conditions prévues au paragraphe 12.a.i – à savoir que la notification « [peut être soumise] à l'application de restrictions proportionnées autorisées par son cadre juridique interne, nécessaires [...] pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée ».

254. De manière générale, les Parties sont encouragées à inclure dans cette notification, en vertu du paragraphe 7.b, et s'il y a lieu, des informations sur le type d'incident de sécurité, la nature et le volume des informations potentiellement compromises, les risques possibles et les mesures envisagées pour limiter les préjudices éventuels, y compris les mesures visant à contenir l'incident. Étant donné la fonction de supervision exercée par les autorités de supervision décrites au paragraphe 14 et afin de bénéficier de conseils d'experts pour la gestion de l'incident, il pourrait également être utile que la Partie qui émet la notification informe ces autorités de l'incident et des mesures d'atténuation prises le cas échéant.

255. Pour permettre une réponse coordonnée et y contribuer dans le cadre de ses propres mesures d'atténuation du risque, la Partie destinataire de la notification peut demander des consultations et des informations supplémentaires au sujet de l'incident et des mesures prises par la Partie émettrice de la notification pour y remédier.

256. Le paragraphe 7.c établit la procédure requise pour la désignation par les Parties de l'autorité ou des autorités auxquelles notification doit être faite en vertu du paragraphe 7.b aux fins du chapitre II, section 2.

Paragraphe 8 – Tenue des registres

257. Le paragraphe 8 impose aux Parties de « [tenir] des registres ou se dote[r] d'autres moyens appropriés pour montrer comment il est accédé aux données personnelles d'un individu, et comment celles-ci sont utilisées et divulguées dans un cas spécifique ». L'objectif est que chaque Partie dispose de moyens effectifs pour démontrer de quelle manière il a été accédé aux données à caractère personnel d'une personne spécifique et comment ces données ont été utilisées et divulguées dans ce cas précis, conformément au présent article. Il est important, en particulier à des fins de contrôle, de montrer que les règles ont été respectées, ce qui contribue en soi à la responsabilité. Si les moyens à mettre en œuvre pour montrer comment sont traitées les données sont laissés à la discrétion de chaque Partie, les Parties sont encouragées à adapter leurs méthodes aux circonstances, en tenant compte des risques pour les personnes concernées et de la nature, de l'étendue, des finalités et du contexte global de ce traitement.

258. Certaines Parties peuvent, par exemple, décider d'utiliser l'enregistrement automatisé des activités (log) ou d'autres solutions (comme la consignation manuelle dans le cas de dossiers papier). Comme indiqué ci-dessus, l'objectif est de favoriser la responsabilité tout en permettant une certaine souplesse quant à la manière dont une Partie remplit cet objectif, dans le respect des autres obligations applicables en vertu de l'article 14. Ainsi, les Parties devraient tenir des registres ou disposer d'autres documents relatifs à l'accès aux données, à leur utilisation ou à leur divulgation sous une forme qui facilite le travail des autorités de supervision.

Paragraphe 9 – Partage ultérieur au sein d'une Partie

259. Le paragraphe 9 dispose que « [l]orsqu'une autorité d'une Partie fournit des données à caractère personnel reçues initialement en vertu du présent Protocole à une autre autorité de cette Partie, cette dernière les traite

conformément au présent article, sous réserve du paragraphe 9.b ». En d'autres termes, lorsque des données à caractère personnel reçues en vertu du présent Protocole sont ensuite communiquées à une autre autorité de la même Partie – y compris à une autorité d'un État constituant ou d'une autre entité territoriale similaire –, ces données doivent être traitées conformément au présent article, à moins que l'exception prévue au paragraphe 9.b s'applique. Le paragraphe 9 s'applique aussi en cas de partage ultérieur multiple.

260. Le paragraphe 9.b prévoit une exception au paragraphe 9.a dans le cas où un État fédéral partie au présent Protocole émet une réserve portant sur les obligations visées à l'article 17 du Protocole, conformément aux conditions fixées par cet article. En accord avec le paragraphe 298 du présent rapport explicatif, cette exception a pour but de prendre en compte « les difficultés que des États fédéraux risquent de rencontrer en raison de la répartition typique des pouvoirs entre les autorités fédérales et régionales », qui correspond au paragraphe 316 du rapport explicatif de la Convention. Par conséquent, le paragraphe 9.b dispose qu'une Partie qui a émis une réserve au titre de l'article 17 conserve la possibilité de communiquer des données à caractère personnel reçues en vertu du présent Protocole à ses États constituants ou autres entités territoriales similaires à condition qu'elle ait mis en place des mesures afin que les autorités destinataires continuent de protéger efficacement ces données en assurant un niveau de protection des données comparable à celui offert par le présent article. Une partie qui n'aurait pas « mis en place des mesures pour que les autorités qui reçoivent les données continuent à les protéger efficacement en assurant un niveau de protection des données comparable à celui offert par le présent article » se trouverait, en fonction de la gravité, des raisons et des circonstances du manquement à cette obligation, en situation de violation flagrante ou systématique du paragraphe 15 de l'article 14.

261. Le paragraphe 9.c prévoit que la Partie transférante est fondée, en cas d'indications selon lesquelles le présent paragraphe ne serait pas correctement appliqué par une autre Partie, à demander une consultation à cette autre Partie et des informations pertinentes sur ces indications afin de clarifier la situation.

Paragraphe 10 – Transfert ultérieur vers un autre État ou vers une organisation internationale

262. Aux termes du paragraphe 10.a, une Partie n'est autorisée à transférer des données à caractère personnel reçues en vertu du présent Protocole « à un autre État ou à une organisation internationale qu'avec l'autorisation préalable de l'autorité qui les lui a communiquées ou, aux fins de la section

2 du chapitre II, de l'autorité ou des autorités désignées en vertu du paragraphe 10.b ». Ce type de mesure conservatoire est une condition courante encadrant les transferts et dont le but est d'assister les partenaires étrangers dans le contexte de l'application du droit pénal (par exemple en vertu de traités d'entraide judiciaire ou de la coopération entre polices) ; cette approche est reprise dans le présent paragraphe également comme un moyen de protéger les données à caractère personnel transférées en vertu du présent Protocole.

263. Le paragraphe 10.b dispose que chaque Partie doit, au moment de la signature ou lors du dépôt de l'instrument de ratification de ce Protocole, d'acceptation ou d'approbation, indiquer au Secrétaire Général du Conseil de l'Europe quelles sont l'autorité ou les autorités désignées pour donner l'autorisation visée au paragraphe 10.a aux fins des transferts en vertu de la section 2 du chapitre II ; les autorités ainsi désignées peuvent être modifiées par la suite.

264. L'obtention d'une autorisation de transfert ultérieur peut nécessiter l'envoi d'une demande individualisée par les autorités de la Partie transférante aux autorités de la Partie requérante en vue du transfert de données à caractère personnel spécifiées à un pays tiers ou à une organisation internationale donnée. Toutefois, le paragraphe 10.a n'empêche pas les Parties de fixer à l'avance les règles régissant les transferts ultérieurs (par exemple par voie d'un accord écrit ou selon d'autres modalités). Le paragraphe 10.a ne fait pas non plus obstacle à la possibilité pour une Partie de fixer d'autres conditions pour l'utilisation de données par le destinataire (comme des limites à l'usage ou à la diffusion par la Partie destinataire de données à caractère personnel afin d'éviter de nuire à l'enquête menée par la Partie transférante) conformément aux dispositions spécifiques du chapitre II.

265. Lorsqu'elle statue sur une demande de transfert en vertu du paragraphe 10, l'autorité transférante ou désignée est encouragée à tenir dûment compte de tous les facteurs pertinents, comme la gravité de l'infraction pénale, le but dans lequel les données ont été transférées à l'origine, les conditions applicables au transfert originel et le niveau approprié ou non de protection des données à caractère personnel garanti par le pays tiers ou l'organisation internationale concernée.

Paragraphe 11 – Transparence et notification

266. Le paragraphe 11.a impose des conditions de transparence et de notification aux Parties pour les éléments visés aux paragraphes 11.a.i à iv. Ces conditions de transparence et de notification ont pour but d'aider les personnes

concernées à comprendre comment les Parties peuvent être amenées à traiter leurs données. Elles sont aussi destinées à informer les personnes concernées des possibilités d'accès, de rectification et de recours existantes.

267. Chaque Partie dispose d'une latitude pour décider si ces notifications et cette transparence sont assurées par voie de publication de notifications générales à l'attention du public – par exemple sur un site internet gouvernemental – ou par notification personnelle à la personne dont les données à caractère personnel ont été adressées à la Partie destinataire. Ces notifications doivent être facilement accessibles et compréhensibles. Qu'elles soient générales ou personnelles, les notifications doivent comporter les informations suivantes: (i) le fondement légal du traitement et ses finalités, y compris les buts de la divulgation anticipée ou habituelle ; (ii) les durées de conservation ou de révision en vertu du paragraphe 5 du présent article ; le cas échéant, (iii) les destinataires ou catégories de destinataires auxquels les données sont divulguées et iv. les possibilités d'accès, de rectification et de recours judiciaires et non judiciaires existantes.

268. Aux termes du paragraphe 11.b, lorsque la notification est adressée personnellement à la personne dont les données ont été transférées à la Partie destinataire, les conditions de notification et de transparence visées au paragraphe 11.a peuvent faire l'objet de restrictions raisonnables conformément aux conditions énoncées au paragraphe 12.a.i du présent article. Ainsi, en matière pénale, il peut y avoir des circonstances légitimes justifiant de différer ou d'omettre la notification. Ces circonstances sont évoquées au paragraphe 12.a.i et décrites au paragraphe 272 du présent rapport explicatif. Il peut aussi se produire des situations dans lesquelles le niveau de détail de la notification générale peut être limité, en fonction de la sensibilité des informations.

269. Le paragraphe 11.c offre aux Parties une base d'appréciation pour mettre en balance le souci de transparence et la nécessaire confidentialité dans les affaires pénales. Il dispose que, lorsque le cadre juridique interne de la Partie transférante impose que toute personne dont les données ont été transférées à une autre Partie en vertu du présent Protocole en reçoive personnellement la notification, la Partie transférante prend toutes les mesures nécessaires pour que la Partie destinataire soit informée de cette obligation au moment du transfert et des coordonnées nécessaires. La Partie transférante ne donne pas notification du transfert de données à la personne concernée si la Partie destinataire demande que ce transfert reste confidentiel, lorsque les conditions de restriction fixées au paragraphe 12.a.i s'appliquent. Lorsque de telles conditions aux restrictions ne s'appliquent plus et que notification personnelle

peut être donnée à l'intéressé, la Partie destinataire prend des mesures pour que la Partie transférante soit informée que la notification peut être faite. Ces mesures peuvent comprendre un réexamen périodique de l'utilité de ces restrictions. Si elle n'en a pas été informée, la Partie transférante est fondée à adresser des demandes à la Partie destinataire, qui l'informerait s'il convient de maintenir la restriction.

Paragraphe 12 – Accès et rectification

270. Le paragraphe 12.a impose à chaque Partie de garantir que toute personne dont elle a reçu les données à caractère personnel en vertu du présent Protocole a le droit de demander et d'obtenir l'accès à ces données, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif (ce droit pouvant faire l'objet d'éventuelles restrictions), et de les faire rectifier lorsque ces données sont inexactes ou ont fait l'objet d'un traitement indu. L'expression « conformément aux procédures établies dans son cadre juridique interne » donne aux Parties une certaine souplesse quant à la manière dont l'accès aux données et leur rectification peuvent être demandés et obtenus. L'intention est de renvoyer à des procédures établies, par exemple, par des lois, réglementations, règles (de nature juridictionnelle notamment) et politiques en vigueur ainsi qu'aux règles applicables en matière d'établissement de la preuve. Dans certains systèmes juridiques, la personne concernée devra d'abord chercher à obtenir le droit d'accès et de rectification au niveau administratif avant de passer par la voie judiciaire.

271. Le paragraphe 12.a.i dispose que la personne qui dépose une demande d'accès a le droit d'obtenir une copie écrite ou électronique de la documentation contenant ses données à caractère personnel ainsi que les informations disponibles relatives au fondement juridique et aux finalités du traitement de ces données, de leur conservation et de leurs destinataires ou catégories de destinataires (« l'accès »), ainsi que des informations relatives aux possibilités de recours conformément au paragraphe 13. Cela peut également permettre à l'individu de confirmer si (ou non) ses données personnelles ont été reçues en vertu du Protocole, et ont été ou sont traitées. La communication de la documentation contenant les informations disponibles indiquant le fondement juridique et les finalités du traitement des données aidera la personne concernée à déterminer si les données à caractère personnel sont traitées conformément à la législation applicable. Dans de nombreuses Parties, le cadre prévoyant l'accès à ces informations peut déjà être fourni par leur législation relative à la vie privée, à la liberté d'information ou à l'accès aux dossiers administratifs.

272. L'obtention de cet accès peut, dans des cas particuliers, être soumise à des restrictions proportionnées autorisées par le cadre juridique interne d'une Partie, ces restrictions devant être « nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et [tenir] dûment compte des intérêts légitimes de la personne concernée ». Les droits et libertés d'autrui peuvent, par exemple, comprendre la vie privée d'autres personnes dont les données à caractère personnel seraient révélées si l'accès était accordé. Les objectifs d'intérêt public général importants peuvent, par exemple, être la protection de la sûreté nationale et de la sécurité publique (ce qui concerne, par exemple, les informations relatives à des menaces terroristes potentielles ou à des risques sérieux pour les membres des forces de l'ordre), la prévention, la détection, l'instruction ou la poursuite d'infractions pénales et la nécessité d'éviter de nuire aux enquêtes, informations judiciaires et procédures officielles. Dans ce contexte, les « restrictions proportionnées » doivent être appliquées par chaque Partie conformément aux principes correspondants de son ordre juridique interne, dans un sens analogue à celui donné dans l'explication du principe de proportionnalité au paragraphe 146 du rapport explicatif de la Convention. Pour les Parties à la Convention européenne des droits de l'homme et au Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, la proportionnalité découlera des obligations imposées par ces conventions. Les autres parties appliqueront les principes correspondants de leur ordre juridique interne qui limitent raisonnablement la possibilité d'obtenir l'accès pour protéger d'autres intérêts légitimes. Comme indiqué ci-dessus, 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. Dans les cas où ces motifs de restriction sont invoqués, l'autorité requise est encouragée à étayer cette décision aux fins du paragraphe 14. Les Parties devraient également considérer la possibilité d'accorder un accès partiel lorsque les motifs de restriction (par exemple dans le but de protéger des informations commerciales confidentielles ou classifiées) ne s'appliquent qu'à certaines parties des informations concernées.

273. Lorsque d'autres dispositions de cet article permettent des restrictions dans les conditions exposées au paragraphe 12.a.i, l'expression « au moment de la décision » renvoie, dans le cas du paragraphe 7, au moment de la notification de l'incident de sécurité et, dans le cas du paragraphe 11.b, au moment

de l'envoi de la notification de transfert des données à caractère personnel ; et dans le cas du paragraphe 11.c, au moment où une Partie demande la confidentialité.

274. En vertu du paragraphe 12.a.ii, chaque Partie veille à ce que toute personne dont les données ont été reçues en application du présent Protocole ait le droit de demander et d'obtenir, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif, la rectification de ses données à caractère personnel, conformément aux procédures établies en droit interne et sans délai indu, lorsque ces données sont inexactes ou ont été indûment traitées. Cette rectification consistera notamment – selon ce qui convient et ce qui est raisonnable au vu des motifs justifiant la rectification et le contexte particulier du traitement – à corriger les données, à les compléter (par exemple par des annotations, des informations complémentaires ou des corrections), à les effacer ou à les anonymiser, à en restreindre le traitement ou à les bloquer. À cet égard, les rédacteurs ont considéré que l'effacement ou l'anonymisation est la solution appropriée et raisonnable dans le cas où les données sont traitées en violation du paragraphe 5. En cas de violation du paragraphe 2, il peut aussi être approprié que la Partie restreigne le traitement ; cependant, cela dépendra en fin de compte du contexte particulier (par exemple de la nécessité de conserver les données à caractère personnel aux fins de l'établissement de la preuve). Lorsque les données sont anonymisées, les Parties devraient prendre en considération le risque d'une réidentification non autorisée et envisager d'appliquer des mesures appropriées pour limiter autant que possible ce risque. Les Parties sont encouragées à notifier, lorsque c'est possible, à la Partie transférante et aux autres entités auxquelles les données ont été communiquées toutes les mesures de rectification prises.

275. Aux termes du paragraphe 12.b, en cas de refus ou de limitation de l'accès ou de la rectification visés au paragraphe 12.a, la Partie informe la personne concernée de ce refus ou de cette limitation par écrit, y compris par voie électronique, et sans retard indu. Si l'autorité doit motiver ce refus ou cette limitation, la communication peut être générale (c'est-à-dire qu'elle peut ne pas confirmer ou dénier l'existence d'un dossier correspondant) dans les cas où cela est nécessaire pour ne pas compromettre un objectif, conformément au paragraphe 12.a.i. Les Parties doivent cependant veiller à ce que cette communication donne des informations sur les possibilités de recours existantes.

276. Les Parties peuvent facturer des frais d'accès (par exemple pour les coûts administratifs liés à la compilation et à l'examen de documents auxquels l'accès

a été demandé). Toutefois, les frais éventuels doivent rester dans les limites du raisonnable et ne pas être excessifs au vu des ressources impliquées afin de ne pas dissuader ou décourager les intéressés de faire une demande d'accès. Pour faciliter l'exercice des droits énoncés au paragraphe 12.a, les Parties sont encouragées à autoriser les personnes concernées à se faire assister par un représentant pour demander et obtenir les mesures qui y sont décrites ou pour déposer une demande et/ou une réclamation en leur nom. Dans ces circonstances, les notifications faites en application du paragraphe 11.a ainsi que les informations obtenues en réponse à une demande d'accès en vertu du paragraphe 12.a.i pourront mentionner cette possibilité. Cette représentation doit cependant être conforme aux conditions prescrites par le droit interne applicable de la Partie à laquelle ces mesures sont demandées, ou la requête et/ou la plainte est déposée comme décrit ci-dessus, notamment pour ce qui est des conditions dans lesquelles des personnes ou entités peuvent représenter les intérêts légaux de tiers (comme les règles régissant la procuration dans certains systèmes juridiques nationaux).

Paragraphe 13 – Recours judiciaire et non judiciaire

277. Le paragraphe 13 dispose que « [c]haque partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article ». Il appartient à chaque Partie de déterminer les types de recours ouverts pour les violations des dispositions de cet article. Il n'est pas obligatoire que chaque type de recours soit ouvert pour chaque violation de cet article. Les voies de recours prévues pour remédier aux violations du présent article doivent être effectives. Les Parties peuvent prévoir, lorsque la situation s'y prête, le dédommagement comme moyen de réparation de préjudices matériels ou non matériels pour lesquels le plaignant a établi qu'ils résultent de la violation concernée.

Paragraphe 14 – Supervision

278. Le paragraphe 14 exige des Parties qu'elles « dispose[nt] d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et effectives à l'égard des mesures établies dans le présent article ». Cette disposition laisse aux Parties toute latitude sur la manière de mettre en œuvre cette obligation. Certaines pourront établir des autorités spécialisées dans la protection des données tandis que d'autres pourront choisir de faire exercer cette supervision concurremment par plusieurs autorités, dont les fonctions peuvent

se recouper, reflétant ainsi les différences de structures constitutionnelles, organisationnelles et administratives entre les Parties. Dans certaines d'entre elles, ces autorités de supervision pourront être établies au sein des structures gouvernementales dont elles supervisent les activités, leur budget faisant partie du budget global de ces structures. Dans ce cas, ces autorités devraient jouir de l'indépendance nécessaire pour pouvoir s'acquitter effectivement de leurs responsabilités de supervision.

279. Les rédacteurs ont considéré que plusieurs éléments contribuent à l'indépendance et à l'effectivité des fonctions et compétences de supervision. Ainsi, ces autorités devraient remplir leur mission et exercer leurs compétences de manière impartiale. Elles devraient pouvoir agir en étant dégagées de toute influence extérieure susceptible d'interférer dans l'exercice indépendant de leurs fonctions et compétences. Elles ne devraient, en particulier, recevoir aucune instruction, dans une affaire donnée, portant sur l'exercice de leurs compétences en matière d'enquête et/ou sur la prise de mesures correctives. Enfin, il est important qu'elles disposent des compétences, des connaissances et de l'expertise nécessaires pour mener à bien leurs tâches et qu'elles soient dotées des ressources financières, techniques et humaines appropriées pour pouvoir exercer effectivement leurs fonctions.

280. Les fonctions et compétences de ces autorités « comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives ». Les rédacteurs ont considéré que les pouvoirs d'enquête devraient inclure le pouvoir d'obtenir les informations nécessaires pour que ces autorités puissent mener à bien leurs tâches, notamment l'accès, sous réserve des conditions appropriées, aux registres tenus en vertu du paragraphe 8. Les actions correctives pourront inclure des avertissements en cas de non-conformité ou des consignes pour assurer la conformité des opérations de traitement des données (exigeant par exemple la mise en œuvre de mesures supplémentaires de sécurité pour limiter l'accès aux données ou la rectification de données à caractère personnel), l'imposition de la suspension (temporaire) de certaines opérations de traitement, ou le renvoi de la question à d'autres autorités (par exemple à des services d'inspection générale, des procureurs, des juges d'instruction ou des instances législatives). Ces mesures correctives peuvent être prises de la propre initiative des autorités ou à la suite de plaintes déposées par des personnes concernant le traitement de leurs données à caractère personnel.

281. Les Parties sont encouragées à promouvoir la coopération entre leurs autorités de surveillance respectives. Des 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. Cela peut inclure l'échange d'informations et de meilleures pratiques.

Paragraphe 15 – Consultation et suspension

282. Le paragraphe 15 régit les situations dans lesquelles une Partie est fondée, aux termes de l'article 14 à suspendre le transfert de données à caractère personnel à une autre Partie en vertu du présent Protocole lorsque les Parties agissent en application du paragraphe 1.a de l'article 14. Étant donné l'importance des finalités répressives du présent Protocole, le paragraphe 15 établit clairement que cette suspension ne devrait intervenir que dans le cadre de conditions strictes et conformément aux procédures spécifiques qu'il décrit. Le but des dispositions de l'article 14 relatives à la protection des données est d'offrir les garanties appropriées pour la protection des données à caractère personnel, y compris lorsqu'elles font ensuite l'objet d'un partage avec d'autres instances au sein d'une même Partie et d'autres transferts. Les rédacteurs ont considéré que les garanties apportées par cet article et leur mise en œuvre effective sont essentielles et qu'il est donc important de prévoir la suspension des transferts de données à caractère personnel dans certaines situations. En conséquence, une Partie peut suspendre le transfert vers une autre Partie de données à caractère personnel effectué en vertu du présent Protocole s'il a des preuves substantielles d'une violation systématique ou flagrante des termes du présent article ou de l'imminence d'une violation flagrante. Si la condition de la « preuve substantielle » n'impose pas à une Partie de démontrer l'existence indubitable d'une violation systématique ou flagrante, cette Partie ne peut pas suspendre les transferts en se fondant sur de simples soupçons ou conjectures. Sa décision doit bien plutôt être solidement fondée sur des éléments de preuve factuels crédibles. Une « violation flagrante » est une violation consécutive d'une obligation importante au titre de cet article. Il peut s'agir de l'absence, dans le cadre juridique interne d'une Partie, d'une garantie requise en vertu de cet article. Les rédacteurs ont reconnu que la suspension est aussi possible en raison de violations systématiques, par exemple de violations fréquentes des garanties apportées par cet article. Ils ont en outre reconnu que la non-application de certaines garanties lors du traitement de données à caractère personnel dans un cas donné ne constitue pas une raison suffisante, en l'absence d'une violation flagrante, pour invoquer cette disposition car la personne concernée devrait pouvoir demander réparation de ces violations par des voies de recours judiciaires et non judiciaires effectives en vertu du paragraphe 13 de l'article 14.

283. Le paragraphe 15 dispose en outre que « [c]ette suspension n'interviendra qu'à l'expiration d'un préavis raisonnable et après que les Parties auront mené des consultations d'une durée raisonnable sans parvenir à une solution ». Cette obligation de consultations dispose que la suspension de transferts essentiels à des fins de répression ne devrait intervenir qu'après avoir donné à l'autre Partie une possibilité raisonnable de clarifier la situation ou de remédier aux inquiétudes exprimées. À l'ouverture de ces consultations, la Partie qui invoque le paragraphe 15 peut demander à l'autre Partie de lui fournir les informations pertinentes. Toutefois, comme le reconnaît le paragraphe 15, la Partie qui invoque ce paragraphe doit disposer de preuves substantielles d'une violation flagrante ou systématique ou de l'imminence d'une violation flagrante. Le mécanisme de consultations ne doit donc pas être utilisé pour collecter d'autres preuves lorsqu'il n'y a que des soupçons de violation. Les transferts de données effectués en vertu du présent Protocole ne peuvent être suspendus qu'après un préavis raisonnable et l'échec de consultations d'une durée raisonnable. Toutefois, une Partie peut suspendre provisoirement les transferts en cas de violation systématique ou flagrante présentant un risque important et imminent pour la vie ou la sécurité d'une personne physique ou de préjudice financier ou de réputation pour cette personne. Est également visée l'existence d'un risque important et imminent de préjudice pour l'intégrité corporelle ou la santé d'une personne physique. Dans ces cas, la Partie adresse une notification à l'autre Partie et entame des consultations avec elle dès l'application de la suspension provisoire des transferts. Les rédacteurs ont considéré que la suspension provisoire devrait, de manière générale, être limitée aux transferts directement concernés par les motifs justifiant la suspension provisoire.

284. Si la Partie qui procède à la suspension remplit les conditions fixées au paragraphe 15, elle peut suspendre les transferts sans que l'autre Partie puisse faire de même. Toutefois, si cette autre Partie a la preuve substantielle que la suspension n'était pas conforme aux termes du paragraphe 15, elle peut à son tour suspendre les transferts vers la Partie qui a décidé la suspension. Dans ce contexte, l'expression « preuve substantielle » a le même sens que dans le cas de la suspension initiale. La suspension décidée par la première Partie serait incompatible avec le paragraphe 15 dans le cas où cette Partie n'a pas de « preuve substantielle », que la violation n'est ni « systématique » ni « flagrante » ou que cette Partie n'a pas satisfait aux conditions procédurales de la suspension, en particulier pour ce qui est des consultations.

285. Enfin, le paragraphe 15 dispose que « la Partie qui a procédé à la suspension lève cette dernière dès qu'il a été remédié à la violation justifiant la

suspension » et que « toute suspension réciproque est levée à ce moment ». Une règle similaire à celle prévue à l'article 24, paragraphe 4, s'applique en cas de suspension en vertu du présent paragraphe, à savoir que « toutes les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au présent Protocole ».

286. Les Parties sont encouragées à notifier officiellement aux fournisseurs de services et aux entités auxquels des demandes ou des injonctions peuvent être adressées en vertu de la section 2 du chapitre II toute suspension ou suspension provisoire en vertu du présent paragraphe ou à rendre publiques ces demandes ou ces injonctions. Cette communication peut être importante pour suspendre effectivement les transferts de données à caractère personnel à une Partie qui viole systématiquement ou de manière flagrante l'article 14, mais aussi pour assurer que les fournisseurs de services et les entités ne limitent pas le transfert d'informations ou de preuves en vertu du présent Protocole parce qu'ils pensent à tort qu'une Partie fait l'objet d'une suspension provisoire.

287. Bien que le paragraphe 15 prévoie des procédures spécifiques relatives aux consultations et à la suspension des transferts de données à caractère personnel pour des raisons de protection des données, ces procédures n'ont pas pour but de modifier les dispositions de l'article 23, paragraphe 1, relatives aux consultations, ni les droits de suspension qui peuvent être applicables à d'autres articles du présent Protocole en vertu du droit international.

Chapitre IV – Clauses finales

288. Les dispositions du présent chapitre s'inspirent essentiellement à la fois du « Modèle de clauses finales pour les conventions, protocoles additionnels et protocoles d'amendement conclus au sein du Conseil de l'Europe », qui a été adopté par le Comité des Ministres lors de la 1291^e réunion des Délégués des Ministres tenue en juillet 2017, et des clauses finales de la Convention. Étant donné que certains des articles du présent chapitre reprennent le libellé du modèle de clauses ou s'inspirent de la longue pratique conventionnelle du Conseil de l'Europe, ils n'appellent pas de commentaires particuliers. Toutefois, certaines modifications du modèle de clauses et des clauses finales de la Convention sur la cybercriminalité méritent une explication.

Article 15 – Effets de ce Protocole

289. Le paragraphe 1.a de l'article 15 incorpore l'article 39, paragraphe 2, de la Convention. Ce paragraphe dispose que les Parties sont libres d'appliquer

des accords préexistants ou qui pourraient entrer en vigueur à l'avenir, comme le reconnaît le paragraphe 312 du rapport explicatif de la Convention. Le Protocole, tout comme la Convention, pose généralement des obligations minimales ; par conséquent, ce paragraphe reconnaît que les Parties sont libres de souscrire des obligations plus spécifiques, en plus de celles déjà fixées dans le Protocole, lorsqu'elles établissent leurs relations au sujet des questions traitées dans ce dernier. Toutefois, les Parties sont tenues, ce faisant, de respecter les objectifs et principes du Protocole et ne peuvent donc accepter d'obligations qui iraient à l'encontre du but de ce dernier.

290. Le paragraphe 1.b de cet article reconnaît aussi l'intégration accrue de l'Union européenne depuis l'ouverture de la Convention à la signature, en 2001, en particulier dans les domaines de la coopération policière et judiciaire en matière criminelle et de la protection des données. Il autorise, par conséquent, les États membres de l'Union européenne à appliquer entre eux le droit de l'Union européenne qui régit les questions traitées par le Protocole. Pour les rédacteurs, le droit de l'Union européenne s'entend des mesures, principes et procédures prévues par l'ordre juridique de l'Union, en particulier ses lois, règlements et dispositions administratives, ainsi que les autres mesures contraignantes, dont les décisions de justice. Le but du paragraphe 1.b est donc de couvrir les relations internes entre les États membres de l'Union européenne, et entre ses États membres, ses institutions, ses organes et ses agences. En l'absence de dispositions législatives de l'Union européenne sur une question entrant dans le champ d'application du présent Protocole, celui-ci continuerait de régir la question concernée entre les Parties qui sont membres de l'Union.

291. Le paragraphe 1.c précise que le paragraphe 1.b ne porte nullement atteinte à la pleine application du présent Protocole entre les Parties qui sont membres de l'Union et d'autres Parties. Le paragraphe 1.b n'a donc pas pour but de produire un quelconque effet au-delà des relations internes à l'Union telles que décrites au paragraphe 290 ci-dessus. Le Protocole s'applique pleinement entre les Parties qui sont membres de l'Union et les autres Parties. Les rédacteurs ont jugé cette disposition essentielle pour garantir que les Parties qui ne sont pas membres de l'Union bénéficieraient pleinement du Protocole dans leurs relations avec des Parties qui sont des États membres de l'Union européenne. Ainsi, les rédacteurs ont débattu du fait de savoir si un État membre de l'Union qui reçoit des informations ou des preuves d'une Partie qui n'est pas membre de l'Union devrait chercher à obtenir le consentement de cette dernière avant de transférer les informations ou preuves en question à une

autre Partie membre de l'Union, conformément à l'article 14, paragraphe 10. De même, le paragraphe 1.a de cet article s'appliquerait pleinement entre les Parties qui sont membres de l'Union et les Parties qui ne le sont pas.

292. Le paragraphe 2 de l'article 15 incorpore l'article 39, paragraphe 3, de la Convention. Pas plus que la Convention, comme cela est exposé au paragraphe 314 du rapport explicatif de la Convention, le présent Protocole n'a pour but de traiter toutes les questions concernant les diverses formes de coopération entre les Parties ou entre les Parties et des entités privées en matière de cybercriminalité et de collecte de preuves d'infractions pénales sous forme électronique. Par conséquent, le paragraphe 2 de l'article 15 a été inséré pour qu'il soit clair que le Protocole n'a d'effet que sur les questions dont il traite. Il ne saurait avoir d'incidence sur les autres droits, restrictions, obligations et responsabilités qui peuvent exister mais que le Protocole ne règle pas.

293. L'article 15 ne comporte pas de disposition analogue à l'article 39, paragraphe 1, de la Convention. Cette disposition de la Convention explique que l'objet de la Convention était de compléter des traités ou accords bilatéraux applicables entre les Parties, notamment certains traités d'extradition et d'entraide. Le présent Protocole ne comprend aucune disposition d'extradition et nombre de ses dispositions ne concernent pas l'entraide. Comme exposé plus en détail à l'article 5 et dans son rapport explicatif correspondant, les modes d'interaction entre chacune des sections du chapitre II relatives aux mesures de coopération et les traités d'entraide sont variables. Par conséquent, les rédacteurs ont estimé qu'il était inutile d'inclure une disposition analogue à celle de l'article 39, paragraphe 1.

Article 16 – Signature et entrée en vigueur

294. L'article 16 autorise toutes les Parties à la Convention à signer le présent Protocole et à devenir Parties à ce dernier. À la différence du Premier Protocole (article 11), le présent Protocole ne prévoit pas de procédure d'adhésion au présent Protocole. Un État souhaitant signer le présent Protocole et devenir Partie à ce dernier devra d'abord devenir Partie à la Convention.

295. Le paragraphe 3 dispose que le présent « Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Parties à la Convention auront exprimé leur consentement à être liées par le présent Protocole. » Alors que l'article 36, paragraphe 3, de la Convention prévoyait qu'au moins trois des cinq Parties devaient être des

États membres du Conseil de l'Europe pour que la Convention entre en vigueur, cette condition n'est pas prévue ici car il s'agit d'un protocole additionnel à une convention et toutes les Parties doivent avoir le même droit d'appliquer le présent Protocole dès qu'un nombre minimal de cinq Parties à la Convention auront exprimé leur consentement à être liés par lui. C'est l'approche suivie par l'article 10 du Premier Protocole.

296. Le paragraphe 4 décrit le processus d'entrée en vigueur du présent Protocole pour les Parties à la Convention qui exprimeront leur consentement à être liées par ce dernier après son entrée en vigueur conformément au paragraphe 3. C'est l'approche suivie par l'article 36, paragraphe 4, de la Convention.

Article 17 – Clause fédérale

297. L'article 17 du présent Protocole comporte une clause fédérale analogue à celle de l'article 41 de la Convention, qui permet à un État fédéral partie au Protocole de formuler une réserve pour assurer la cohérence avec « [les] principes fondamentaux régissant les relations entre son gouvernement central et les États constitutants ou autres entités territoriales similaires ». Le but de l'article 17 est le même que celui de l'article 41 de la Convention, qui est, comme exposé au paragraphe 316 du rapport explicatif de la Convention, « de trouver un arrangement concernant les difficultés que des États fédéraux risquent de rencontrer en raison de la répartition typique des pouvoirs entre les autorités fédérales et régionales ».

298. Les États fédéraux sont autorisés à faire des réserves concernant les obligations découlant du chapitre II de la Convention (établissement des infractions pénales et des mesures procédurales en droit interne) lorsque ces mesures ne relèvent pas des compétences du gouvernement central de l'État fédéral. Toutefois, il est attendu des États fédéraux qu'ils soient en mesure d'offrir une coopération internationale aux autres Parties en vertu du chapitre III de la Convention.

299. Bien que le présent Protocole porte sur la coopération internationale plutôt que sur des mesures de droit interne, les négociateurs ont reconnu qu'il restait nécessaire d'y faire figurer une clause fédérale. Alors que la Convention ne prévoit pas la possibilité de faire des réserves liées au fédéralisme en matière d'entraide judiciaire, la majorité des mesures prévues par le présent Protocole ne fonctionnent pas de la même manière que dans le cadre de l'entraide classique. Le Protocole prévoit plusieurs mesures de coopération d'une efficacité

supérieure à l'entraide classique et qui ne nécessitent pas forcément de passer par le gouvernement central. Il introduit en particulier deux mesures, aux articles 6 et 7, permettant aux autorités compétentes d'une Partie de chercher à coopérer directement avec des entreprises privées établies dans une autre Partie. Ces dispositions nécessitent le respect de certaines mesures procédurales qu'un État fédéral pourrait avoir du mal à imposer aux autorités compétentes d'États constituants ou d'autres entités territoriales similaires. Ainsi, l'article 7 prévoit qu'une Partie peut, moyennant notification au Secrétaire Général, exiger des autorités d'autres Parties qu'elles avisent immédiatement une autorité gouvernementale désignée à cet effet de toute injonction adressée à un fournisseur de services pour obtenir des informations relatives aux abonnés. D'autres articles imposent de prendre des mesures législatives ou autres qu'un État fédéral peut ne pas être en situation de pouvoir exiger de ses États constituants ou entités territoriales similaires. Enfin, le présent Protocole comprend des dispositions détaillées relatives à la protection des données, ce qui n'est pas le cas de la Convention. Aux États-Unis par exemple, en vertu de la Constitution et des principes fondamentaux du fédéralisme, les États constituants adoptent leurs propres lois pénales et lois de procédure pénale (distinctes des lois fédérales) ; ils établissent leurs propres tribunaux, procureurs et services de police et conduisent les enquêtes et poursuites concernant les infractions à leur législation pénale. Les autorités compétentes des États sont indépendantes des autorités fédérales, auxquelles elles ne sont pas subordonnées.

300. Lorsque les autorités d'un État constituant ou d'une entité territoriale similaire d'un État fédéral souhaitent bénéficier des formes de coopération prévues par le présent Protocole, il se peut : 1. que leurs lois procédurales et relatives à la protection de la vie privée diffèrent de celles appliquées par les autorités du gouvernement central ; 2. qu'elles ne soient pas soumises hiérarchiquement au gouvernement central ; ou 3. que le gouvernement central n'ait pas légalement compétence pour diriger leurs actions. Dans ces situations, la seule assurance qu'il pourrait y avoir qu'un État constituant ou une entité territoriale similaire se conforme aux prescriptions du présent Protocole – en ce qui concerne la collecte d'informations ou de preuves ainsi que leur traitement subséquent – serait : a. qu'il les applique lui-même ou b. que ses autorités cherchent à obtenir la coopération par l'intermédiaire des autorités du gouvernement central, ou avec leur participation, lesquelles veilleraient alors au respect de ces obligations (par exemple par le biais de l'entraide ou du point de contact du Réseau 24/7, ou par la participation du gouvernement central à une ECE).

301. Au vu de ces considérations, le paragraphe 1 prévoit une possibilité pour les États fédéraux parties au Protocole de faire des réserves. Ils peuvent se réserver le droit d'assumer les obligations découlant du présent Protocole conformément à leurs principes fondamentaux régissant les relations entre leur gouvernement central et leurs États constituants ou autres entités territoriales similaires, sous réserve des paragraphes 1.a à c, qui limitent la portée de ces réserves. En vertu du paragraphe 1.a, le gouvernement central d'un État fédéral qui fait une telle réserve est tenu d'appliquer toutes les dispositions du présent Protocole (sans préjudice des réserves et déclarations possibles). Dans le cas des Parties pour lesquelles les obligations relatives à la protection des données prévues par le présent Protocole sont régies par l'article 14, paragraphe 1.a, cela comprend les obligations énoncées à l'article 14, paragraphe 9.b, relatives au partage des données avec des États constituants ou d'autres entités territoriales similaires (voir le paragraphe 260 du rapport explicatif) lorsqu'une autorité fédérale a demandé des informations en vertu du présent Protocole soit pour ses propres fins, soit pour le compte d'une autorité de niveau inférieur à l'échelon fédéral et partage ensuite ces informations avec cette autorité. De plus, le paragraphe 1.b prévoit, tout comme l'article 41, paragraphe 1, de la Convention que ces réserves sont sans effet sur l'obligation d'un État fédéral partie à la Convention de répondre aux demandes de coopération d'autres Parties conformément aux dispositions du chapitre II. Enfin, en vertu du paragraphe 1.c et sans préjudice des réserves faites par un État fédéral, l'article 13 du présent Protocole – qui exige, conformément à l'article 15 de la Convention, que le droit interne garantisse la protection des droits de l'homme et des libertés – s'applique, outre à l'État fédéral lui-même en vertu du paragraphe 1.a, également aux États constituants ou entités territoriales similaires.

302. Le paragraphe 2 dispose que, dans les cas où un État fédéral fait des réserves en vertu du paragraphe 1 et que les autorités d'un État constituant ou d'une entité territoriale similaire de cette Partie demande la coopération directe d'une autorité, d'un fournisseur de services ou d'une entité située dans une autre Partie, cette dernière « peut empêcher les autorités, les fournisseurs ou les entités sur son territoire de coopérer en réponse à [cette] demande ». Cette autre Partie peut déterminer de quelle manière empêcher les autorités, fournisseurs de services ou entités sur son territoire de coopérer. Il y a deux exceptions à la possibilité d'une Partie d'empêcher la coopération.

303. Premièrement, le paragraphe 2 dispose que la coopération ne peut pas être empêchée par cette autre Partie si l'État fédéral concerné a, du fait que

l'État constituant ou autre entité territoriale similaire remplit les obligations du présent Protocole, « notifié au Secrétaire Général du Conseil de l'Europe que l'État constitutif ou autre entité territoriale similaire s'est engagé à appliquer les obligations du présent Protocole applicables à cet État fédéral ». L'expression « obligations du présent Protocole applicables à cet État fédéral » signifie qu'une autorité d'un État constituant ou autre entité territoriale similaire ne peut être soumise à une obligation auquel le gouvernement central ne serait pas soumis, par exemple en raison d'une réserve applicable. Si l'État fédéral a adressé cette notification au Secrétaire Général pour un État constituant particulier, une autre Partie devra répondre à une injonction ou à une demande de cet État de la même manière que si elle lui avait été adressée par des autorités du gouvernement central. Les obligations et procédures prévues pour chaque mesure de coopération du chapitre II continuent naturellement de s'appliquer aux demandes et injonctions soumises par ces États constituants ou entités territoriales similaires. Le respect de ces obligations est nécessaire. Le paragraphe 2 prévoit que le Secrétaire Général du Conseil de l'Europe établit et tient un registre de ces notifications. Les Parties sont encouragées à communiquer des informations actualisées au Secrétaire Général.

304. Deuxièmement, en vertu du paragraphe 3, si une demande ou une injonction d'un État constituant ou d'une autre entité territoriale similaire a été transmise par l'intermédiaire du gouvernement central ou, aux termes de l'article 12, conformément à un accord d'établissement d'une équipe d'enquête commune auquel participe le gouvernement central, une autre Partie ne peut pas empêcher les autorités, fournisseurs de services ou entités de son territoire de transférer des informations ou des preuves conformément aux dispositions du présent Protocole au motif que la coopération est demandée par un État constituant ou une entité territoriale similaire d'un État fédéral qui a fait des réserves au titre du paragraphe 1. En effet, lorsque la demande ou l'injonction est soumise par l'intermédiaire du gouvernement central ou que l'accord établissant l'équipe commune d'enquête a été conclu avec sa participation, c'est à lui qu'il incombe alors « [d']assurer[r] l'exécution des obligations applicables du Protocole ». Puisque le gouvernement central transmet la demande ou l'injonction (ou participe à l'ECE), il a la possibilité et l'obligation de vérifier le respect des conditions posées par le Protocole en ce qui concerne ces mesures. Ainsi, lorsque notification doit être donnée à une autre Partie, en vertu de l'article 7, paragraphe 5.a, de la transmission d'une injonction pour l'obtention d'informations relatives aux abonnés, c'est au gouvernement central qu'il incombe d'adresser cette notification. En matière de protection des données (pour les Parties auxquelles l'article 14,

paragraphe 1.a, est applicable), lorsqu'un État constituant ou une autre entité territoriale similaire fait une demande de coopération par l'intermédiaire du gouvernement central, celui-ci lui communique les données et est tenu de se conformer aux exigences de l'article 14, paragraphe 9.b (partage des données à l'intérieur d'une Partie). Le gouvernement central doit donc mettre en place des mesures pour que les autorités destinataires des données continuent de les protéger efficacement en assurant un niveau de protection comparable à celui voulu par l'article 14. Les autorités d'un État constituant ou d'une entité territoriale similaire qui demandent et reçoivent des données personnelles de cette manière ne sont sinon pas tenues d'appliquer l'article 14. Si les Parties concernées appliquent un autre accord ou arrangement visé à l'article 14, paragraphes 1.b ou 1.c, les termes applicables de ces accords ou arrangements s'appliquent.

305. Le paragraphe 4 reprend presque à l'identique la formulation de l'article 41, paragraphe 3, de la Convention et a presque les mêmes effets. Ainsi, s'agissant des dispositions de la Convention dont l'application relève de la compétence des États constituant ou autres entités territoriales similaires (sauf notification adressée au Secrétaire Général du Conseil de l'Europe conformément au paragraphe 2 du présent article), le gouvernement central de l'État fédéral est tenu: 1. d'informer les autorités de ses États constituant ou autres entités territoriales similaires des dispositions du présent Protocole ; et 2. de donner « son avis favorable, en les encourageant à prendre les mesures appropriées pour leur donner effet », incitant ainsi les États constituant ou entités territoriales similaires à appliquer pleinement le présent Protocole. Aux fins du Protocole, le but est aussi de permettre finalement que ces États constituant ou autres entités territoriales similaires reçoivent les notifications prévues au paragraphe 2 de cet article.

Article 18 – Application territoriale

306. L'article 38 de ce Protocole permet aux Parties de préciser le ou les territoires auxquels la Convention s'appliquerait. Cet article applique automatiquement le Protocole aux territoires spécifiés par une Partie en vertu de l'article 38, paragraphe 1 ou 2, de la Convention dans la mesure où cette déclaration n'a pas été retirée en vertu de l'article 38, paragraphe 3, de la Convention. Les rédacteurs ont estimé qu'il serait préférable que la Convention et le Protocole aient le même champ d'application territorial comme règle par défaut.

307. Le paragraphe 2 de cet article dispose qu'« [une] Partie peut, au moment de la signature de ce Protocole ou au moment du dépôt de son instrument de

ratification, d'acceptation ou d'approbation, déclarer que le présent Protocole ne s'applique pas à un ou plusieurs territoires spécifiés dans les déclarations de la Partie en vertu des paragraphes 1 et/ou 2 de l'article 38 de la Convention ». Conformément au paragraphe 3, les Parties peuvent retirer la déclaration faite en vertu du paragraphe 2 de cet article, selon les modalités précisées ; le retrait de la déclaration faite au paragraphe 2 aurait pour effet d'appliquer le Protocole à des territoires supplémentaires qui étaient couverts par la Convention mais auxquels le Protocole n'avait pas été appliqué auparavant.

308. Cet article ne permet pas d'appliquer le Protocole aux territoires non couverts par la Convention.

Article 19 – Réserves et déclarations

309. Le présent article prévoit un certain nombre de cas où il est possible de formuler des réserves. Étant donné la portée mondiale de la Convention et le fait qu'il s'agit d'obtenir le même nombre d'adhésions pour le présent Protocole, ces réserves permettent aux Parties à la Convention de devenir Parties au présent Protocole, tout en leur permettant de conserver certaines approches et notions compatibles avec leur législation interne, leurs principes juridiques fondamentaux ou leurs considérations politiques, selon le cas.

310. Les possibilités de faire des réserves sont limitées afin de garantir autant que faire se peut l'application uniforme du présent Protocole par les Parties. C'est pourquoi celles-ci ne peuvent faire aucune autre réserve que celles qui sont énumérées. De plus, une Partie à la Convention ne peut faire une réserve qu'au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

311. Comme pour la Convention, les réserves au présent Protocole visent à exclure ou à modifier l'effet juridique d'obligations énoncées dans le présent Protocole (voir le paragraphe 315 du rapport explicatif de la Convention). Dans le présent Protocole, les réserves sont autorisées à exclure toute une forme de coopération. En particulier, l'article 7, paragraphe 9.a, permet à une Partie de se réserver le droit de ne pas appliquer l'article 7 dans son intégralité. Il est également possible de formuler des réserves pour exclure la coopération concernant tout un article portant sur un certain type de données. C'est ainsi que l'article 7, paragraphe 9.b, autorise une Partie à se réserver le droit de ne pas appliquer l'article 7 à certains types de numéros d'accès si la divulgation de ces numéros devait être incompatible avec les principes fondamentaux de son droit interne.

De même, l'article 8, paragraphe 13, autorise une Partie à se réserver le droit de ne pas appliquer l'article 8 aux données relatives au trafic.

312. L'article 19 porte également sur les déclarations. Comme dans le cas de la Convention, les Parties sont autorisées, par le moyen des déclarations faites dans le cadre du présent Protocole, à insérer certaines procédures supplémentaires spécifiées qui modifient la portée des dispositions. Ces procédures supplémentaires ont pour objet de tenir compte de certaines différences théoriques, juridiques ou pratiques, ce qui se justifie au vu de la portée mondiale de la Convention et de l'aspiration à donner au présent Protocole une portée équivalente. Les déclarations énumérées appartiennent généralement à deux catégories.

313. Plusieurs déclarations autorisent une Partie à déclarer que certains pouvoirs ou mesures doivent être exercés ou appliqués par certaines autorités ou que la coopération doit être assurée par certaines voies. C'est le cas de l'article 10, paragraphe 9 (permettant de déclarer que les demandes peuvent être adressées à des autorités autres que l'autorité centrale) ; de l'article 12, paragraphe 3 (l'autorité centrale doit être signataire de l'accord de l'ECE ou y adhérer d'une autre manière) ; de l'article 8, paragraphe 11 (une Partie faisant une déclaration peut exiger que les demandes des autres Parties soumises en vertu de cet article soient transmises par les autorités centrales ou par toute autre autorité déterminée d'un commun accord).

314. Les déclarations appartenant à la deuxième catégorie autorisent les Parties à exiger la prise de mesures procédurales distinctes ou supplémentaires concernant certaines mesures de coopération afin de respecter le droit interne ou d'empêcher que les autorités ne soient submergées. Ainsi, par exemple, l'article 7, paragraphe 8, et l'article 9, paragraphe 1.b, autorisent une Partie à faire des déclarations tendant à exiger la prise de certaines mesures procédurales concernant les données relatives aux abonnés. L'article 7, paragraphes 2.b et 5.a, l'article 8, paragraphe 4, et l'article 9, paragraphe 5, autorisent la prise de mesures procédurales supplémentaires pour fournir des garanties supplémentaires ou respecter la législation interne. Les déclarations ne sont pas destinées à être réciproques. Ainsi, par exemple, si une Partie fait une déclaration en vertu de l'article 10, paragraphe 9 – tendant à ce que les demandes soumises en application de cet article puissent être adressées aux autorités ainsi qu'à son autorité centrale –, les autres Parties peuvent adresser les demandes aux autorités supplémentaires de la Partie ayant fait la déclaration, mais cette dernière ne peut qu'adresser les demandes aux autorités centrales des autres Parties, à moins qu'elles ne fassent elles aussi une déclaration en ce sens.

315. Les déclarations visées au paragraphe 2 doivent être faites au moment de la signature par une Partie ou lorsque celle-ci dépose son instrument de ratification, d'acceptation ou d'approbation. En revanche, les déclarations visées au paragraphe 3 peuvent être faites à tout moment.

316. Le paragraphe 3 fait obligation aux Parties de notifier au Secrétaire Général du Conseil de l'Europe toute déclaration, notification ou communication visée à l'article 7, paragraphe 5.a et e, et à l'article 8, paragraphes 4 et 10.a et b, à l'article 14, paragraphe 7.c et 10.b, et à l'article 17, paragraphe 2 du présent Protocole conformément aux conditions spécifiées dans ces articles. Ainsi, par exemple, en vertu de l'article 7, paragraphe 5.e, une « Partie doit, au moment où la notification prévue au paragraphe 5.a est adressée pour la première fois au Secrétaire Général du Conseil de l'Europe, communiquer à ce dernier les coordonnées de cette autorité. » De plus, les Parties communiquent au Secrétaire Général du Conseil de l'Europe les « autorités » visées à l'article 8, paragraphe 10.a et b. Il a été demandé au Secrétaire Général de créer et de tenir à jour un registre de ces autorités désignées par les Parties, et il est demandé à celles-ci de veiller à tout moment à l'exactitude des informations qui y sont consignées (voir l'article 7, paragraphe 5.f, et l'article 8, paragraphe 12).

Article 20 – Statut et retrait des réserves

317. Comme l'article 43 de la Convention, cet article, sans imposer de délais spécifiques, exige des Parties qu'elles retirent leurs réserves dès que les circonstances le permettent. Afin de pouvoir exercer une certaine pression sur les Parties en vue de les amener au moins à envisager de retirer leurs réserves, le paragraphe 2 autorise le Secrétaire Général du Conseil de l'Europe à s'enquérir périodiquement des perspectives de retrait desdites réserves. Cette possibilité de demander des renseignements, devenue pratique courante dans le cadre de l'application de plusieurs instruments du Conseil de l'Europe, se retrouve à l'article 43, paragraphe 3, de la Convention et à l'article 13, paragraphe 2, du Premier Protocole. Les Parties peuvent ainsi indiquer si elles doivent maintenir leurs réserves au sujet de certaines dispositions et retirer ultérieurement celles qui sont devenues inutiles. On espère qu'avec le temps les Parties pourront retirer autant de réserves que possible de façon à promouvoir l'application uniforme du présent Protocole.

Article 21 – Amendements

318. Le présent article suit la même procédure que celle que prévoit l'article 44 de la Convention pour les amendements. Cette procédure simplifiée permet,

en cas de besoin, d'apporter des amendements sans avoir à négocier un protocole d'amendement. Il est entendu que les consultations des Parties à la Convention, prévues au paragraphe 3 du présent article, ont un caractère non contraignant pour les Parties au Protocole. Comme indiqué au paragraphe 323 du rapport explicatif de la Convention, « (o)n considère que la procédure d'amendement s'applique pour l'essentiel à des modifications relativement mineures à caractère procédural ou technique ».

Article 22 – Règlement des différends

319. L'article 22 permet que les mécanismes de règlement des différends prévu à l'article 45 de la Convention s'appliquent également au présent Protocole (voir le paragraphe 326 du rapport explicatif de la Convention).

Article 23 – Concertation des Parties et évaluation de l'application

320. Le paragraphe 1 de l'article 23 prévoit que l'article 46 de la Convention (Concertation des Parties) est applicable au présent Protocole. Conformément au paragraphe 327 du rapport explicatif de la Convention, l'article 46 a institué « un cadre devant permettre aux Parties de se concerter au sujet de la mise en œuvre de la Convention, des répercussions des nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique ou en relation avec l'ordinateur, et de la collecte de preuves sous forme électronique, ainsi que de l'éventualité de compléter ou d'amender la Convention ». La procédure a été conçue pour être souple: il appartient aux Parties de décider comment ou quand se rencontrer. Après l'entrée en vigueur de la Convention en 2004, les Parties ont commencé à se rencontrer régulièrement dans le cadre du « Comité de la Convention sur la cybercriminalité » (T-CY). Au fil du temps, le T-CY, créé en application de l'article 46 et se conformant au règlement intérieur adopté par les Parties à la Convention, a procédé à des évaluations de l'application de la Convention par les Parties, adopté des notes d'orientation devant favoriser une interprétation commune par les Parties des modalités d'application de la Convention et élaboré le projet du présent Protocole. Les procédures à suivre au titre de la concertation des Parties à ce Protocole conservent leur souplesse et peuvent donc être adaptées par celles-ci, s'il y a lieu, pour tenir compte de besoins que l'application du présent Protocole pourrait faire apparaître.

321. Comme pour la Convention (voir rapport explicatif, paragraphe 327), les consultations prévues à l'article 23 devraient « examiner les questions qui se sont posées lors de l'utilisation et de la mise en œuvre de la Convention,

y compris les effets des déclarations et réserves formulées ». Cela pourrait inclure des consultations et une évaluation de la mise en œuvre du Protocole par les États constitutifs ou les entités territoriales similaires des États fédéraux notifiés au Secrétaire Général du Conseil de l'Europe en vertu de l'article 17, paragraphe 2, et, pour les Parties qui sont membres de l'Union, l'information et la consultation des autres Parties au Protocole sur la législation de l'Union applicable à l'utilisation et à la mise en œuvre du Protocole en vertu de l'article 15, paragraphe 1.b. Outre les consultations par le biais du T-CY en vertu de cet article, examinées dans le paragraphe suivant, les Parties peuvent engager des consultations sur une base bilatérale. Pour les États fédéraux, ces consultations et évaluations se dérouleraient par l'intermédiaire de leur gouvernement central.

322. Le paragraphe 2 de l'article 23 établit des procédures spécifiques pour examiner l'utilisation et la mise en œuvre du Protocole dans le cadre plus large établi par l'article 46 et le T-CY mentionné ci-dessus. Le paragraphe 2 prévoit que « les Parties évaluent périodiquement l'utilisation et la mise en œuvre effectives des dispositions du présent Protocole » et indique que l'article 2 du Règlement intérieur établi par le T-CY, tel que révisé le 16 octobre 2020, régira ces évaluations. Ces procédures sont disponibles sur le site web du T-CY. Puisque le T-CY a examiné plusieurs dispositions de la Convention et a publié des rapports conformément à ces procédures, les rédacteurs ont considéré que ces procédures bien établies s'appliquaient, *mutatis mutandis*, à l'évaluation des dispositions du présent Protocole. Compte tenu des obligations supplémentaires contractées par les parties à ce protocole et des mesures de coopération uniques qu'il prévoit, les rédacteurs ont décidé que seules les parties au protocole procéderaient à ces évaluations. Compte 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.

323. Les règles régissant ces évaluations doivent certes être prévisibles, mais l'expérience concrète peut imposer d'adapter ces procédures, sans que soit requis un amendement formel du présent Protocole en vertu de l'article 21. En conséquence, le paragraphe 2 indique que les Parties réexaminent et peuvent modifier ces procédures par consensus cinq ans après l'entrée en vigueur de l'instrument, date à laquelle les Parties pourront modifier ces procédures par consensus. Les parties peuvent modifier les procédures par consensus à tout moment après cet examen initial.

324. Étant donné l'importance des garanties de protection de données de l'article 14, les rédacteurs ont été d'avis que le présent article devait être évalué dès que le niveau de coopération atteint dans le cadre du présent Protocole permet d'examiner utilement l'usage et la mise en œuvre de cette disposition. C'est pourquoi le paragraphe 3 dispose que l'évaluation de l'article 14 commencera une fois que 10 Parties auront exprimé leur consentement à être liés par ce Protocole.

Article 24 – Dénonciation

325. Les paragraphes 1 et 2 de l'article 24 sont analogues à ceux du paragraphe 47 de la Convention et ne nécessitent aucune explication supplémentaire. Le paragraphe 3 stipule que « [l]a dénonciation de la Convention par une Partie au présent Protocole constitue une dénonciation du présent Protocole ». Étant donné que le présent Protocole met l'accent sur le partage d'informations ou de preuves pouvant inclure des données à caractère personnel, les rédacteurs ont jugé prudent d'ajouter le paragraphe 4 pour préciser que « [l]es informations ou éléments de preuve transférés avant la date de prise d'effet de la dénonciation continuent d'être traités conformément au présent Protocole ».

Notes d'orientation

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies¹⁶.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La Convention « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »¹⁷, et ce pour que de nouvelles formes de délits soient toujours couvertes par la Convention.

Note d'orientation sur la notion de « système informatique »

Article 1.a de la Convention de Budapest sur la cybercriminalité

Adoptée par le T-CY lors de sa 8^e réunion plénière (5-6 décembre 2013)

1. Introduction

Lors de sa première réunion à Strasbourg, les 20 et 21 mars 2006, le T-CY s'est penché sur la portée de l'expression « système informatique » telle qu'elle se trouve définie à l'article 1.a de la Convention de Budapest, compte tenu des nouvelles formes de technologie qui vont au-delà des simples ordinateurs de bureau ou ordinateurs centraux traditionnels.

Depuis 2004, date à laquelle la Convention a été rédigée, de nouveaux dispositifs sont apparus, avec notamment la génération moderne des téléphones portables dits « smartphones », les ordinateurs de poche (PDA), les tablettes et autres, qui permettent de produire, traiter ou transmettre des données. D'où la nécessité de voir si la notion de « système informatique » qu'utilise la Convention de Budapest couvre ces nouveaux dispositifs.

16. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

17. Paragraphe 36 du rapport explicatif.

Le T-CY a décidé, en 2006, que les dispositifs en question étaient couverts par la définition du « système informatique » qui figure à l'article 1.a de la Convention.

La présente note d'orientation consacre cette interprétation commune des Parties, telle qu'elle ressort du rapport de la 1^{re} réunion (document T-CY(2006)11).

2. Article 1.a de la Convention de Budapest sur la cybercriminalité (STCE no 185)

Texte de la Convention

Article 1 – Définitions

Aux fins de la présente Convention,

a. l'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

Extrait du Rapport explicatif

23. Aux fins de la Convention, un système informatique est un dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau. « Automatisé » signifie sans intervention humaine directe, le « traitement des données » est un ensemble d'opérations appliquées à des données et effectuées par le biais de l'exécution d'un programme informatique. Un « programme informatique » est un ensemble d'instructions pouvant être exécutées par l'ordinateur pour obtenir le résultat attendu. Un ordinateur peut exécuter différents programmes. Dans un système informatique, on distingue généralement plusieurs composantes, à savoir le processeur ou l'unité centrale, et les périphériques. Par « périphérique », on entend un dispositif qui remplit certaines fonctions spécifiques en interaction avec l'unité centrale : imprimante, écran, lecteur/graveur de CD-Rom ou autre moyen de stockage, par exemple.

24. Un réseau est une interconnexion entre deux systèmes informatiques ou plus. Les connexions peuvent être reliées à la terre (fil ou câble, par exemple), sans fil (radio, infrarouge ou satellite, par exemple), ou les deux. Un réseau peut être géographiquement limité à une zone peu étendue (réseau local) ou couvrir une zone étendue (réseau étendu), et de tels réseaux peuvent eux-mêmes être interconnectés. L'Internet est un réseau mondial composé de nombreux réseaux interconnectés, qui utilisent tous les mêmes protocoles. Il existe encore d'autres types de réseaux, connectés ou non à l'Internet, capables de faire circuler des

données entre des systèmes informatiques. Les systèmes informatiques peuvent être connectés au réseau en tant que points de sortie ou comme moyen de faciliter la transmission de l'information (routeurs et dispositifs similaires, par exemple). L'important, c'est que les données soient échangées sur le réseau.

3. Déclaration du T-CY concernant la notion de « système informatique » (article 1.a de la Convention de Budapest)

L'article 1.a de la Convention définit un « système informatique » comme « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ».

Le T-CY considère que cette définition englobe, par exemple, les téléphones portables modernes, qui sont des appareils multifonctionnels capables de produire, traiter et transmettre des données, leurs multiples fonctions consistant notamment à accéder à l'internet, à envoyer des courriers électroniques, à joindre et transmettre des fichiers, ainsi qu'à télécharger des contenus ou documents.

De même, le T-CY a conscience que les assistants numériques personnels (PDA), qu'ils soient ou non équipés de la fonctionnalité sans fil, peuvent eux aussi produire, traiter et transmettre des données.

Le T-CY souligne que, lorsque ces dispositifs exécutent de telles fonctions, ils traitent des « données informatiques » au sens de l'article 1.b. Il considère par ailleurs qu'ils génèrent aussi, ce faisant, des « données relatives au trafic » au sens de l'article 1.d.

Dès lors qu'ils traitent de telles données, les dispositifs en question se comportent comme un « système informatique » au sens de l'article 1.a.

Le T-CY estime qu'une telle acception est conforme à l'interprétation que donne du « système informatique » le rapport explicatif de la Convention et que cette dernière a vocation à couvrir ces dispositifs dans leur utilisation en tant que tel.

4. Conclusion

Le T-CY considère que la définition du « système informatique » qui figure à l'article 1.a couvre de nouvelles formes de technologie qui vont au-delà des simples ordinateurs de bureau ou ordinateurs centraux, avec notamment les téléphones portables modernes, les « smartphones », les assistants numériques personnels, les tablettes et autres appareils similaires.

Note d'orientation sur les dispositions de la Convention de Budapest visant les botnets

Adoptée lors de la 9^e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies ¹⁸.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note traite de la question des botnets.

La Convention « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »¹⁹, et ce pour que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux botnets.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE no 185)

Le terme « botnet » peut désigner :

« un groupe d'ordinateurs qui ont été contaminés par des logiciels malveillants (virus informatiques). Un tel réseau d'ordinateurs compromis ("zombies") peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les "zombies" peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé "centre de commande et de contrôle" »²⁰.

18. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

19. Paragraphe 36 du rapport explicatif.

20. Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre du Conseil 2005/222/JAI (COM (2010) 517 final).

Des ordinateurs peuvent être reliés entre eux à des fins criminelles ou pour de bonnes causes²¹. Le fait que les botnets soient constitués d'ordinateurs reliés entre eux n'est donc pas un critère pertinent. L'élément essentiel est que les ordinateurs des botnets sont utilisés sans autorisation, à des fins criminelles et pour causer des dégâts majeurs.

Les botnets sont visés par certains articles de la Convention, en fonction de l'action précise qu'ils accomplissent. Ces articles sont énumérés ci-dessous. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.), dont la preuve devrait être apportée sans difficulté en présence de botnets.

Articles pertinents	Exemples
Article 2 – Accès illégal	La création et l'exploitation d'un botnet nécessitent un accès illégal à des systèmes informatiques ²² . Les botnets peuvent servir à accéder illégalement à d'autres systèmes informatiques.
Article 3 – Interception illégale	Les botnets peuvent utiliser des moyens techniques pour intercepter des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	La création d'un botnet altère toujours et peut endommager, effacer, dégrader ou supprimer des données informatiques. Les botnets eux-mêmes endommagent, effacent, dégradent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les botnets peuvent entraver le fonctionnement d'un système informatique, notamment au moyen d'attaques par déni de service distribué ²³ .

21. Des réseaux d'ordinateurs peuvent être sciemment créés à des fins criminelles. Les infractions commises par ces réseaux sont couvertes par la Convention, mais ne sont pas examinées dans la présente note.

22. Voir également la note d'orientation n° 1 relative à la notion de « système informatique ».

23. Voir la note d'orientation sur ce sujet.

Articles pertinents	Exemples
Article 6 – Abus de dispositifs	Les botnets sont tous des dispositifs relevant de la définition figurant à l'article 6, car ils sont conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5 ²⁴. Les programmes utilisés pour créer et exploiter des botnets entrent aussi dans le champ de l'article 6. Par conséquent, l'article 6 érige en infractions pénales la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mises à disposition des dispositifs que sont les botnets ou les programmes utilisés pour leur création ou leur exploitation.
Article 7 – Falsification informatique	Selon la façon dont il a été conçu, le botnet peut introduire, altérer, effacer ou supprimer des données informatiques, engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.
Article 8 – Fraude informatique	Les botnets peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 9 – Pornographie enfantine	Les botnets peuvent diffuser des contenus qui relèvent de l'exploitation d'enfants.
Article 10 – Atteinte à la propriété intellectuelle et aux droits connexes	Les botnets peuvent diffuser illégalement des données qui sont protégées par les lois relatives à la propriété intellectuelle.

24. Les Parties qui émettent des réserves concernant l'article 6 doivent néanmoins toujours ériger en infraction pénale la vente, la diffusion ou la mise à disposition de dispositifs visés par ledit article.

Articles pertinents	Exemples
Article 11 – Tentative et complicité	Les botnets peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complice de leur commission.
Article 13 – Sanctions	Les botnets sont utilisés à de multiples fins criminelles, dont certaines ont une incidence grave sur les personnes, les institutions publiques ou privées ou les infrastructures essentielles. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux botnets soit trop clémentine et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux botnets « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les botnets portent atteinte à un nombre important de systèmes ou que les attaques causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

2. Déclaration du T-CY

La liste des articles concernant les botnets présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen des botnets et les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que les botnets, sous leurs différents aspects, sont couverts par la Convention de Budapest.

Note d'orientation sur les attaques DDOS

Adoptée lors de la 9^e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en œuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies²⁵.

Les notes d'orientation reflètent la vision commune de toutes les Parties quant à l'utilisation de la Convention.

La présente note est consacrée à la question des attaques par déni de service (DOS) et par déni de service distribué (DDOS).

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »²⁶, et ce pour que les nouvelles formes de logiciels malveillants ou d'infractions soient toujours couvertes par la Convention.

La présente note montre dans quelle mesure plusieurs articles de la Convention s'appliquent aux attaques DOS et DDOS.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE no 185)

Les attaques DOS visent à rendre un système informatique indisponible pour ses utilisateurs par divers moyens, dont la saturation des ordinateurs ou réseaux ciblés par des demandes de communication externes, qui ralentit l'accès au service pour les utilisateurs légitimes. Les attaques DDOS sont des attaques par déni de service exécutées par plusieurs ordinateurs en même temps. Il existe actuellement plusieurs manières de lancer des attaques DOS et DDOS, par exemple envoyer des requêtes incorrectes à un système informatique, dépasser le nombre maximal d'utilisateurs ou envoyer un nombre de courriers électroniques supérieur à celui que le serveur peut recevoir et traiter.

25. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

26. Paragraphe 36 du rapport explicatif.

Les attaques DOS et DDOS sont visées par certains articles de la Convention, en fonction de ce qu'elles accomplissent. Ces articles sont énumérés ci-dessous. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.), dont la preuve devrait être apportée sans difficulté en cas d'attaque DOS ou DDOS.

2. Interprétation par le T-CY de la criminalisation des attaques DDOS

Articles pertinents	Exemples
Article 2 – Accès illégal	Par le biais des attaques DOS et DDOS il est possible d'accéder à un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les attaques DOS et DDOS peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Une attaque DOS ou DDOS vise précisément à entraver gravement le fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les attaques DOS et DDOS peuvent être utilisées pour tenter de commettre plusieurs des infractions spécifiées dans la Convention ou pour se rendre complice de leur commission (telles que la falsification informatique, article 7 ; la fraude informatique, article 8 ; les infractions se rapportant à la pornographie infantine, article 9, et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes, article 10).
Article 13 – Sanctions et mesures	Les attaques DOS et DDOS peuvent être dangereuses de multiples façons, en particulier lorsqu'elles sont dirigées contre des systèmes qui sont essentiels au quotidien – par exemple, si un système bancaire ou hospitalier est rendu indisponible. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux attaques DOS et DDOS soit trop clémente et ne permette pas la prise en considération de circonstances aggravantes, de la tentative ou de la complicité.

Articles pertinents	Exemples
	D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux attaques DOS et DDOS « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques DOS ou DDOS portent atteinte à un nombre important de systèmes ou causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

3. Déclaration du T-CY

La liste des articles concernant les attaques DOS et DDOS présentée ci-dessus

illustre les multiples infractions qui peuvent être commises au moyen de ces

attaques.

Par conséquent, le T-CY estime que les différents aspects de ces attaques sont

couverts par la Convention de Budapest.

Note d'orientation sur la fraude par usurpation d'identité et hameçonnage

Adoptée lors de la 9^e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8^e session plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, y compris à la lumière des nouveautés juridiques, politiques ou techniques²⁷.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question de la fraude par usurpation d'identité et hameçonnage (« phishing ») ou par des pratiques analogues²⁸.

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »²⁹. Cela vise à garantir que les nouvelles formes de criminalité seront toujours couvertes par la Convention.

Cette note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent à l'usurpation d'identité par voie informatique en lien avec la fraude.

1. Usurpation d'identité et hameçonnage

Il n'existe pas de définition universellement acceptée de ce qui constitue une usurpation d'identité. Malgré le caractère fluctuant de l'usage de cette notion, on entend communément par « usurpation d'identité » des infractions pénales qui consistent à obtenir et à utiliser de façon frauduleuse (à son insu et sans son consentement) les données personnelles d'une autre personne. Le terme « fraude à l'identité » est parfois employé comme synonyme, bien

27. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

28. Ces pratiques sont connues sous des appellations diverses : spear phishing ou « harponnage », SMiShing, pharming et vishing.

29. Paragraphe 36 du rapport explicatif.

que cette notion englobe également le fait d'utiliser une fausse identité, qui n'est pas forcément réelle.

Les renseignements personnels d'une personne réelle ou fictive peuvent être utilisés à mauvais escient pour commettre de nombreux actes illicites. La présente note d'orientation ne traite cependant que des usurpations d'identité liées à la fraude.

Cela peut impliquer l'appropriation frauduleuse d'informations relatives à l'identité (par exemple nom, date de naissance, adresse actuelle ou adresses antérieures) d'une autre personne, à son insu et sans son consentement. Ces renseignements personnels sont ensuite utilisés pour obtenir des biens et services en son nom.

Ce type d'agissements peut prendre plusieurs formes comme le « phishing », le « pharming », le « spear phishing », le « spoofing » ou toute autre conduite analogue visant, par exemple, à obtenir un mot de passe ou d'autres clés d'accès, souvent par le biais de courriers électroniques ou de sites web falsifiés.

L'usurpation d'identité est un véritable fléau qui touche les gouvernements, les entreprises et les citoyens. Ce phénomène mine la confiance dans les technologies de l'information.

La plupart des systèmes juridiques ne prévoient pas de délit spécifique d'usurpation d'identité. Les auteurs d'usurpation d'identité sont normalement inculpés de délits plus graves (comme la fraude financière). L'obtention d'une fausse identité implique normalement la commission d'une infraction, comme la falsification de documents ou l'altération de données informatiques. Une fausse identité facilite la perpétration de nombreux crimes dont l'immigration illégale, la traite des êtres humains, le blanchiment d'argent, le trafic de drogue et la fraude financière contre les gouvernements et le secteur privé, mais est généralement associée à la fraude.

Sur le plan conceptuel, une usurpation d'identité peut se décomposer en trois étapes :

- Phase 1 – L'obtention des renseignements personnels par des moyens divers tels que le vol physique, l'utilisation de moteurs de recherche, des attaques de l'intérieur ou de l'extérieur (accès illicite aux systèmes informatiques, Trojans, « keyloggers », logiciels espions et autres programmes malveillants), ou bien par le recours au hameçonnage ou à d'autres techniques d'ingénierie sociale.

- Phase 2 – La possession et la cession des renseignements personnels (par exemple, la vente de ces informations à des tiers).
- Phase 3 – L'utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions, par exemple en prenant l'identité d'une autre personne pour exploiter des comptes en banque ou des cartes de crédit, ouvrir de nouveaux comptes, contracter des prêts et crédits, commander des biens et services ou diffuser des programmes malveillants.

En conclusion : l'usurpation d'identité (y compris le hameçonnage et les conduites analogues) sert généralement à la préparation de nouveaux agissements criminels, comme la fraude informatique. Bien que l'usurpation d'identité ne constitue pas une infraction en elle-même, les services chargés de l'application des lois peuvent engager des poursuites pour les infractions connexes.

2. Interprétation de la pénalisation de la fraude par usurpation d'identité donnée par le T-CY au regard de la Convention de Budapest

La Convention de Budapest traite avant tout des actes criminels et n'aborde pas expressément les techniques ou technologies employées. En conséquence, elle ne contient pas de dispositions spécifiques relatives à l'usurpation d'identité ou au hameçonnage. Cependant, la pleine application des dispositions de droit matériel de la Convention permet aux Etats d'ériger en infraction pénale tout agissement lié à une usurpation d'identité.

La Convention fait obligation aux Etats d'ériger en infraction pénale des agissements tels que l'accès illégal à un système informatique, l'interception illégale de données, l'atteinte à l'intégralité des données, l'atteinte à l'intégralité du système, l'abus de dispositifs et la falsification informatique :

Phases	Articles de la Convention	Exemples
Phase 1 – Obtention des renseignements personnels	Article 2 – Accès illégal	Lorsqu'un pirate contourne la protection par mot de passe, enregistre les frappes d'un clavier (« keylogging ») ou exploite les failles des logiciels, il est possible d'accéder illégalement à l'ordinateur à des fins d'usurpation d'identité ou de hameçonnage. L'accès illégal aux systèmes informatiques figure parmi les infractions les plus communément commises pour obtenir des données sensibles, comme les renseignements personnels.
	Article 3 – Interception illégale	L'usurpation d'identité comporte souvent le recours à des dispositifs de surveillance (« key-loggers ») ou autres types de programmes malveillants pour intercepter illégalement des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique contenant des données sensibles, comme les renseignements personnels.
	Article 4 – Atteinte à l'intégrité des données	L'usurpation d'identité ou le hameçonnage peuvent endommager, effacer, dégrader, altérer ou supprimer des données informatiques. Cela intervient souvent dans le cadre du processus d'obtention d'un accès illégal, moyennant l'installation d'un « keylogger » pour obtenir des données sensibles.
	Article 5 – Atteinte à l'intégrité du système	L'usurpation d'identité ou le hameçonnage peuvent entraver le fonctionnement d'un système informatique pour voler ou faciliter le vol de données à caractère personnel.

Phases	Articles de la Convention	Exemples
	Article 7 – Falsification informatique	L'usurpation d'identité ou le hameçonnage peuvent donner lieu à l'introduction, l'altération, l'effacement ou la suppression de données informatiques, engendrant des données non authentiques qui seront prises en compte ou utilisées à des fins légales comme si elles étaient authentiques. Le hameçonnage est probablement l'illustration la plus courante d'une falsification informatique (page web falsifiée d'un établissement financier par exemple). Cette activité illicite est par conséquent la méthode la plus couramment employée pour obtenir des données sensibles, comme les renseignements personnels.
Phase 2 – Possession et cession des renseignements personnels	Article 6 – Abus de dispositifs	Les données personnelles volées – mots de passe, clés d'accès, cartes de crédit et autres – peuvent être considérées comme la possession d'un « dispositif, y compris un système informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 » de la Convention ou « d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique ».

Phases	Articles de la Convention	Exemples
Phase 3 – Utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions	Article 8 – Fraude informatique	L'utilisation d'une identité frauduleuse pour introduire, altérer, effacer ou supprimer des données informatiques et/ou porter atteinte au fonctionnement d'un système informatique peut servir à exploiter des prêts et crédits ou commander de biens et services, et peut donc causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique.
Toutes les phases	Article 11 – Tentative et complicité	L'obtention, la possession et la cession de données personnelles peuvent constituer une tentative de commettre plusieurs des infractions spécifiées dans la Convention ou de se rendre complice de leur commission.
	Article 13 – Sanctions	L'usurpation d'identité sert à de multiples fins criminelles dont certaines ont une incidence grave sur les personnes et les institutions publiques ou privées. Il est cependant possible que la sanction prévue par la législation nationale de certaines

Phases	Articles de la Convention	Exemples
		Parties à l'égard de l'usurpation d'identité soit trop clémentes et ne permettent pas la prise en considération des circonstances aggravantes. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à l'usurpation d'identité « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si l'usurpation d'identité porte atteinte à un grand nombre de personnes ou cause un préjudice considérable ou expose une personne à un danger.

3. Déclaration du T-CY

Le T-CY considère que ci-dessus sont illustrées l'étendue et les multiples éléments de pénalisation de l'usurpation d'identité et du hameçonnage ainsi que les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que ces infractions, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

Note d'orientation sur les attaques visant les infrastructures d'information critiques

Adoptée lors de la 9^e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies³⁰.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des attaques visant les infrastructures d'information critiques.

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures³¹. Et ce, afin que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux attaques visant les infrastructures d'information critiques.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE no185)

Les infrastructures critiques désignent en général les systèmes et les actifs, physiques ou virtuels, indispensables à la vie d'un pays et dont le mauvais usage, l'arrêt ou la destruction aurait un effet dévastateur sur la sécurité nationale et la défense, la sécurité économique, la santé ou la sûreté publiques ou n'importe quelle combinaison de ces éléments. La définition des infrastructures critiques varie selon les pays. Toutefois, pour de nombreux pays, les infrastructures critiques englobent l'énergie, l'alimentation, l'eau, les combustibles, les transports, les communications, les finances, l'industrie, la défense et les secteurs des services publics et du gouvernement.

Les infrastructures critiques sont souvent gérées par des systèmes informatiques, notamment ceux connus sous le nom de systèmes de contrôle industriels (SCI) ou de systèmes de télésurveillance et d'acquisition de données (SCADA).

30. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

31. Paragraphe 36 du Rapport explicatif.

Ces systèmes sont généralement désignés sous le nom d’infrastructures d’information critiques.

Selon des sources privées et gouvernementales, un nombre important mais inconnu d’attaques visant des infrastructures d’information critiques se produit chaque année dans le monde entier. Ces attaques ont recours aux mêmes techniques que celles utilisées par la criminalité électronique. La différence réside dans l’impact de ces attaques sur la société: elles peuvent retirer des fonds du Trésor public, interrompre l’approvisionnement en eau, perturber le contrôle du trafic aérien, etc.

Les formes d’attaques des infrastructures d’information critiques, actuelles et futures, sont visées par les articles de la Convention figurant ci-dessous, en fonction de la nature de l’attaque. Chaque disposition contient un critère d’intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

2. Interprétation par le T-CY de l’incrimination des attaques visant des infrastructures d’information critiques

Articles pertinents	Exemples
Article 2 – Accès illégal	Les attaques contre les infrastructures d’information critiques peuvent s’introduire dans un système informatique.
Article 3 – Interception illégale	Les attaques contre les infrastructures d’information critiques peuvent utiliser des moyens techniques pour intercepter des transmissions non publiques de données informatiques, à destination, en provenance ou à l’intérieur d’un système informatique.
Article 4 – Atteinte à l’intégrité des données	Les attaques contre les infrastructures d’information critiques peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l’intégrité du système	Les attaques contre les infrastructures d’information critiques peuvent porter atteinte au fonctionnement d’un système informatique ; il pourrait en fait s’agir de leur objectif premier.

Articles pertinents	Exemples
Article 7 – Falsification informatique	Les attaques contre les infrastructures d'information critiques peuvent introduire, altérer, effacer ou supprimer des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques.
Article 8 – Fraude informatique	Les attaques contre les infrastructures d'information critiques peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les attaques contre les infrastructures d'information critiques peuvent être utilisées pour tenter de commettre des infractions spécifiées dans le traité ou pour se rendre complices de leur commission.
Article 13 – Sanctions	Les incidences des attaques contre les infrastructures d'information critiques sont multiples (elles peuvent varier selon les pays pour des raisons techniques, culturelles ou autres) mais les pouvoirs publics s'y intéressent généralement lorsqu'elles entraînent des préjudices graves ou de grande ampleur. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques contre les infrastructures d'information critiques soit trop clémentine et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ».

Articles pertinents	Exemples
	Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques contre les infrastructures d'information critiques portent atteinte à un nombre important de systèmes ou provoquent des dégâts considérables, y compris des décès ou des blessures physiques.

3. Déclaration du T-CY

La liste des articles concernant les attaques contre les infrastructures d'information critiques présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY s'accorde à dire que ces attaques, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

Note d'orientation sur les nouvelles formes de logiciels malveillants

Adoptée lors de la 9^e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies³².

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des nouvelles formes de logiciels malveillants.

³². Voir le mandat du T-CY (article 46 de la Convention de Budapest).

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures³³. Et ce, afin que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux nouvelles formes de logiciels malveillants.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE no 185)

Il existe actuellement de nombreuses formes de logiciels malveillants. Selon l'Organisation de coopération et de développement économiques « le terme général de « logiciel malveillant » désigne un logiciel introduit dans un système d'information afin de causer des dommages à ce système ou à d'autres systèmes, ou de les destiner à une utilisation autre que celle voulue par leurs utilisateurs légitimes »³⁴. Les formes les plus connues englobent les vers, les virus et les chevaux de Troie. Les logiciels malveillants, sous leurs formes actuelles, peuvent dérober des données en les copiant et en les envoyant vers une autre adresse ; manipuler des données ; porter atteinte au fonctionnement de systèmes informatiques, y compris ceux qui contrôlent des infrastructures critiques ; les « ransomware » peuvent effacer, supprimer ou bloquer l'accès à des données ; et des logiciels malveillants taillés sur mesure peuvent cibler des systèmes informatiques spécifiques.

Selon des sources privées et gouvernementales, de nouvelles formes de logiciels malveillants sont conçues et découvertes en grand nombre chaque année. Leurs objectifs sont variés. Tout comme les formes plus anciennes, les nouvelles formes de logiciels malveillants peuvent voler de l'argent, mettre hors service les systèmes d'approvisionnement en eau, menacer les utilisateurs etc.

Le nombre et la diversité des formes de logiciels malveillants sont tels qu'il serait impossible, même pour les formes connues actuellement, de les définir dans le cadre d'une loi pénale. La Convention sur la cybercriminalité évite délibérément l'utilisation de termes tels que virus, vers et chevaux de Troie. Dans la mesure où la tendance évolue aussi dans le domaine des logiciels

33. Paragraphe 36 du Rapport explicatif.

34. www.oecd.org/internet/ieconomy/40724457.pdf.

malveillants, l'utilisation de ces termes dans la Convention la rendrait rapidement obsolète et contre-productive.

Il est également impossible, bien évidemment, de décrire les formes futures dans une loi.

Pour ces raisons, il importe de se concentrer sur les objectifs et les effets des logiciels malveillants. Ces derniers sont déjà connus et peuvent être visés par une loi.

Par conséquent, les logiciels malveillants, que ce soit sous leur forme actuelle ou leur forme future, sont visés par les articles de la Convention figurant ci-dessous, en fonction de l'action précise qu'ils accomplissent. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

2. Interprétation par le T-CY de l'incrimination des nouvelles formes de logiciel malveillant

Articles pertinents	Exemples
Article 2 – Accès illégal	Les logiciels malveillants peuvent être utilisés pour s'introduire dans des systèmes informatiques.
Article 3 – Interception illégale	Les logiciels malveillants peuvent être utilisés pour intercepter des transmissions non publiques de données informatiques, à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les logiciels malveillants endommagent, effacent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les logiciels malveillants peuvent porter atteinte au fonctionnement d'un système informatique.

Articles pertinents	Exemples
Article 6 – Abus de dispositifs	Les logiciels malveillants sont des dispositifs relevant de la définition figurant à l'article 6 (les Parties qui émettent des réserves quant à l'article 6 doivent néanmoins toujours ériger en infraction la vente, la distribution ou la mise à disposition des dispositifs visés par ledit article). Et ce parce qu'ils sont généralement conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5. Par ailleurs, l'article érige en infraction pénale la vente, l'obtention pour utilisation, l'importation, la distribution ou d'autres formes de mise à disposition de mots de passe, de codes d'accès ou de données similaires permettant de s'introduire dans des systèmes informatiques. L'action pénale à l'encontre des logiciels malveillants met souvent au jour ces éléments.
Article 7 – Falsification informatique	Les logiciels malveillants peuvent introduire, altérer, effacer ou supprimer des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques.
Article 8 – Fraude informatique.	Les logiciels malveillants peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les logiciels malveillants peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complices de leur commission.

Articles pertinents	Exemples
Article 13 – Sanctions	Les incidences des nouvelles formes de logiciels malveillants sont multiples. Certains logiciels malveillants sont relativement anodins ; d'autres présentent un danger pour les personnes, les infrastructures critiques, ou à d'autres niveaux. Les incidences peuvent varier selon les pays pour des raisons techniques, culturelles ou autres. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques perpétrées par des logiciels malveillants soit trop clémentine et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « soient passibles de sanctions effectives, proportionnées et dissuasives comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques de logiciels malveillants portent atteinte à un nombre important de systèmes, provoquent des dégâts considérables, y compris des décès ou des blessures physiques, ou endommagent des infrastructures critiques.

3. Déclaration du T-CY

La liste des articles, présentée ci-dessus, concernant toutes les formes de logiciels malveillants illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY s'accorde à dire que toutes les formes de logiciels malveillants, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

Note d'orientation sur l'accès transfrontalier aux données³⁵

Introduction

Lors de sa 8^e session plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions juridiques, politiques et technologiques.³⁶

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes les Parties.

La présente note est consacrée à la question de l'accès transfrontalier aux données tel que visé à l'article 32 de la Convention de Budapest.³⁷

L'article 32b énonce une exception au principe de territorialité en autorisant dans des circonstances limitées l'accès transfrontalier unilatéral sans passer par l'entraide judiciaire. Les Parties sont invitées à utiliser plus efficacement toutes les dispositions de la Convention de Budapest portant sur la coopération internationale, notamment l'entraide judiciaire.

Dans l'ensemble, les pratiques, les procédures ainsi que les conditions et les garanties qui les accompagnent varient considérablement entre les différentes Parties. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données à caractère personnel, la base légale de l'accès aux données stockées à l'étranger ou au moyen de l'informatique en nuage, et le principe de la souveraineté nationale.

Cette note d'orientation vise à aider les Parties à appliquer la Convention de Budapest, à corriger les malentendus concernant l'accès transfrontalier en vertu de cette convention et à rassurer les tiers.

Elle aidera ainsi les Parties à exploiter pleinement les possibilités offertes par la convention en matière d'accès transfrontalier aux données.

35. Adoptée lors de la 12^e réunion plénière du T-CY (2-3 décembre 2014)

36. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

37. La préparation de cette note d'orientation fait suite aux conclusions du rapport intitulé « Compétence et accès transfrontalier » (T-CY(2012)3) adopté par le T-CY en décembre 2012. [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY\(2012\)3F_transborder_repV31public_7Dec12.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)3F_transborder_repV31public_7Dec12.pdf)

Article 32 de la Convention de Budapest

Texte de l'article :

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

- a. accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou
- b. 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.

Extrait du rapport explicatif :

293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des États agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret ; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. À cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.

294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations : d'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne « légalement autorisée » pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par exemple, le message électronique d'une

personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article.

Interprétation de l'article 32 de la Convention de Budapest par le T-CY

Concernant l'article 32a (accès transfrontalier à des données informatiques accessibles au public ou « données ouvertes »), aucun problème particulier n'a été soulevé et il n'est pour l'instant pas nécessaire que le T-CY donne des orientations supplémentaires.

On considère généralement que les membres des services répressifs peuvent consulter toutes les données accessibles publiquement, et qu'à cette fin ils peuvent s'inscrire ou s'abonner aux services ouverts au public.³⁸

Si une partie d'un site web, d'un service ou d'un système du même type est fermée au public alors que le reste est accessible, cette partie n'est pas considérée accessible au sens de l'article 32a.

Concernant l'article 32b, on peut envisager les situations caractéristiques suivantes :

- Le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services, ou une personne peut stocker délibérément des données dans un autre pays. Cette personne peut récupérer les données et, pourvu qu'elle y soit juridiquement habilitée, elle peut les communiquer de son propre gré aux forces de l'ordre ou leur permettre d'y accéder, tel que prévu à l'article.³⁹
- Un individu suspecté de trafic de drogues est arrêté dans les règles alors que son courrier électronique est ouvert sur sa tablette, son smartphone ou un autre appareil, révélant éventuellement des preuves de délit. Si le suspect autorise de son propre gré la police à accéder à son compte et si celle-ci est certaine que les données sont localisées dans un autre Etat partie, elle peut y avoir accès en vertu de l'article 32b.

38. La législation nationale peut toutefois limiter l'accès à des données publiquement disponibles ou leur utilisation par les services répressifs.

39. Paragraphe 294 du rapport explicatif.

Les autres situations ne sont ni autorisées ni exclues.⁴⁰

Concernant l'article 32b (accès transfrontalier avec consentement), le T-CY partage l'analyse suivante :

Considérations et garanties générales

L'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques dans le cadre de l'article 14.⁴¹

Comme il a été souligné plus haut, les Parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de primauté du droit, conformément à l'article 15 de la Convention de Budapest.⁴²

40. Paragraphe 293 du rapport explicatif. Voir aussi l'article 39.3 de la Convention de Budapest.

41. Article 14 – Champ d'application des mesures procédurales

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2. Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a. aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b. à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c. à la collecte des preuves électroniques de toute infraction pénale.

3. a. Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :

i. qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii. qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

42. Article 15 – Conditions et sauvegardes

1. Chaque 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

Les droits des individus et les intérêts des tiers doivent être pris en compte dans l'application de cette mesure.

Par conséquent, la Partie qui perquisitionne un autre Etat partie peut envisager d'informer les autorités compétentes de celui-ci.

Concernant les notions de « frontière » et de « lieu »

L'accès transfrontalier consiste à « accéder unilatéralement [c'est-à-dire sans passer par l'entraide judiciaire] aux données informatiques stockées sur le territoire d'une autre Partie ». ⁴³

Cette mesure ne peut s'appliquer qu'entre Parties.

L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat [partie] », ce qui signifie qu'il peut être utilisé lorsqu'on sait où les données se trouvent.

L'article 32b ne prévoit pas certaines autres situations, par exemple lorsque les données ne sont pas stockées sur le territoire d'une autre Partie ou lorsqu'on n'a pas la certitude de leur lieu de stockage. Une Partie ne peut invoquer l'article 32b pour obtenir la divulgation de données stockées sur son propre territoire.

Selon l'article 32b, d'autres situations « ne sont ni autorisées ni exclues. » Ainsi, lorsqu'on ignore si les données sont stockées dans un autre Etat partie ou lorsqu'on n'en a pas la certitude, les Parties peuvent être amenées à évaluer elles-mêmes la légitimité d'une perquisition ou d'un autre type d'accès, à la

(Note 41 – Suite)

des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2. Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3. Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

43. Paragraphe 293 du rapport explicatif de la Convention de Budapest

lumière de leur droit interne, des principes applicables de droit international ou des considérations liées aux relations internationales.

Concernant la notion d'« accès sans autorisation de l'autre Partie »

L'article 32b n'impose pas l'utilisation de l'entraide judiciaire, et la Convention de Budapest n'exige pas que l'autre Partie soit informée. Pour autant, la convention n'exclut pas une telle notification. Les Parties peuvent informer l'autre Partie si elles le jugent utile.

Concernant le « consentement »

L'article 32b prévoit que le consentement doit être légal et volontaire, ce qui signifie que la personne qui fournit l'accès aux données ou qui consent à les divulguer ne doit avoir subi ni contrainte ni tromperie.⁴⁴

Selon certaines réglementations nationales, il se peut que les mineurs ou les personnes souffrant de troubles mentaux ou d'autres affections ne puissent donner valablement leur consentement.

Dans la plupart des Etats parties, la coopération dans le cadre d'une enquête pénale requiert un consentement explicite. Par exemple, l'acceptation des conditions générales d'utilisation d'un service en ligne peut être insuffisante à constituer un consentement explicite, même si ces conditions indiquent que les données peuvent être transmises aux autorités judiciaires en cas d'utilisation frauduleuse.

Concernant le droit applicable

Dans tous les cas, les services répressifs doivent appliquer les mêmes normes juridiques dans l'application de l'article 32b que dans leur propre pays. Si l'accès aux données ou leur divulgation ne seraient pas autorisés sur le territoire national, il en va de même dans l'application de l'article 32b.

Les parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de la primauté du droit, conformément à l'article 15 de la Convention de Budapest.

44. Dans certains pays, le fait d'accepter que les poursuites soient abandonnées, ou que la gravité des chefs d'inculpation ou la durée d'une peine de prison soient réduites constitue un consentement légal et volontaire.

Concernant la personne autorisée à fournir l'accès ou à divulguer les données

S'agissant de déterminer « qui » est « légalement autorisé » à divulguer des données, cette question peut varier en fonction des circonstances ainsi que de la législation et de la réglementation en vigueur.

Il peut par exemple s'agir d'un particulier donnant accès à sa messagerie électronique ou à d'autres données qu'il a stockées à l'étranger.⁴⁵

Il peut aussi s'agir d'une personne morale.

Il est peu probable que les prestataires de services remplissent les conditions d'un consentement valide et volontaire concernant la divulgation des données de leurs utilisateurs dans les conditions de l'article 32. En général, les prestataires de services ne sont que les dépositaires de ces données. Ils n'en ont pas le contrôle ni la propriété et ne sont donc pas dans la capacité de donner un consentement valide. En revanche, les forces de l'ordre pourront bien sûr se procurer les données dans un pays étranger par d'autres moyens, comme l'entraide judiciaire ou les procédures applicables aux situations d'urgence.

Demandes internes légalement formulées et article 32b

L'article 32b ne s'applique pas aux injonctions de produire ni à d'autres demandes légalement formulées au sein d'un Etat partie.

Concernant la localisation de la personne consentant à fournir l'accès aux données ou à les divulguer

L'hypothèse habituelle est que la personne qui donne l'accès aux données est physiquement présente sur le territoire de la Partie requérante.

Cependant, de multiples situations sont possibles. On peut envisager que la personne physique ou morale se trouve sur le territoire des services répressifs de l'Etat requérant lorsqu'elle consent à divulguer les données ou à y donner effectivement accès ; ou uniquement lorsqu'elle consent à les divulguer mais pas à y donner accès ; ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle accepte de les divulguer et/ou qu'elle y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle accepte de coopérer ou lorsqu'elle donne effectivement accès aux données. S'il s'agit d'une personne morale, (comme une entité privée), elle peut être

45. Voir l'exemple donné dans le paragraphe 294 du rapport explicatif.

représentée simultanément sur le territoire des services répressifs requérants, sur le territoire où se trouvent les données, voire dans un pays tiers.

Il faut tenir compte du fait que de nombreuses Parties s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des services répressifs étrangers désirant sa coopération; certains pays considèrent même cette démarche comme une infraction pénale.

Déclaration du T-CY

Le T-CY déclare d'un commun accord que la présente note d'orientation reflète une analyse partagée par toutes les Parties quant à l'étendue et aux éléments de l'article 32.

Note d'orientation sur les spams⁴⁶

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies⁴⁷.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des spams. La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »⁴⁸, et ce pour que des formes inédites de logiciels malveillants ou de délits restent malgré tout couvertes par la Convention.

Cette note d'orientation montre comment différents articles de la Convention s'appliquent aux spams.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STE n°185)

Le spam désigne en général l'envoi en masse de courriels non sollicités. Un message est envoyé à un nombre considérable d'adresses électroniques et l'identité personnelle du destinataire n'entre pas en ligne de compte car le message est adressé de la même manière à beaucoup d'autres destinataires, sans distinction.

Des questions distinctes se posent concernant les points suivants :

- le contenu du spam ;
- l'acte d'envoyer un spam, et ;
- le dispositif utilisé pour transmettre un spam.

46. Adoptée lors de la 12^e réunion plénière du T-CY (2-3 décembre 2014)

47. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

48. Paragraphe 36 du rapport explicatif.

Le contenu du spam peut être illégal ou non. Lorsqu'il l'est (comme la proposition de médicaments contrefaits ou des offres financières frauduleuses), l'infraction peut relever de la législation nationale pertinente en la matière. L'acte de transmettre un spam (y compris la transmission à grande diffusion de contenus non répréhensibles) peut constituer une infraction civile ou pénale dans certaines juridictions.

La Convention ne couvre pas les spams dont le contenu n'est pas illégal et ne pas porter une atteinte à l'intégrité du système, mais qui peut-être être nuisibles aux utilisateurs finaux.

Les outils utilisés pour transmettre des spams peuvent être illégaux en vertu de la Convention de Budapest, et les spams peuvent être associés à d'autres infractions qui ne sont pas mentionnées dans le tableau ci-dessous (voir, par exemple, les articles 7 et 8).

Comme pour d'autres notes d'orientation, chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.). Dans certains cas de spams, cette intention peut être difficile à prouver.

Interprétation par le T-CY des dispositions relatives aux spams

Articles pertinents	Exemples
Article 2 – Accès illégal	Les spams peuvent contenir des logiciels malveillants qui peuvent accéder ou permettre d'accéder à un système informatique.
Article 3 – Interception illégale	Les spams peuvent contenir des logiciels malveillants qui peuvent intercepter illégalement ou permettre l'interception illégale de transmissions de données informatiques.
Article 4 – Atteinte à l'intégrité des données	Les spams peuvent contenir des logiciels malveillants qui peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	La transmission de spams peut entraver gravement le fonctionnement des systèmes informatiques. Les spams peuvent contenir des logiciels malveillants qui peuvent entraver gravement le fonctionnement des systèmes informatiques.
Article 6 – Abus de dispositifs	Les dispositifs relevant de la définition figurant à l'article 6 peuvent servir à transmettre des spams. Les spams peuvent contenir des dispositifs relevant de la définition de l'article 6.

Articles pertinents	Exemples
Article 8 – Fraude informatique.	Les spams peuvent servir comme un dispositif d'entrée, de modification, d'effacement ou de suppression de données informatiques ou d'interférence avec le fonctionnement d'un système informatique pour se procurer des avantages économiques illégaux.
Article 10 – Atteinte à la propriété intellectuelle et aux droits connexes	Les spams peuvent servir à faire de la publicité pour la vente de biens contrefaits, notamment des logiciels ou d'autres éléments protégés par les lois relatives à la propriété intellectuelle.
Article 11 – Tentative et complicité	Les spams et la transmission de spams peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans la Convention ou pour se rendre complice de leur commission (telles que la falsification informatique, article 7 ; la fraude informatique, article 8).
Article 13 – Sanctions	Les spams peuvent être utilisés à de multiples fins criminelles, dont certaines ont une incidence grave sur les personnes, ou les institutions publiques ou privées. Si une Partie n'érige pas en infraction pénale le spam en tant que tel, elle devrait ériger en infraction pénale tout agissement lié aux spams tel que les infractions susmentionnées, et permettre la prise en considération de circonstances aggravantes, de la tentative ou de la complicité. Les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux spams « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris de sanctions pécuniaires.

Déclaration du T-CY

La liste des articles présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen des spams et les infractions liées aux spams.

Par conséquent, le T-CY s'accorde à dire que les spams, sous leurs différents aspects, sont couverts par la Convention de Budapest.

Note d'orientation sur les injonctions de produire concernant des informations sur les abonnés (Article 18 de la Convention de Budapest)⁴⁹

Introduction

A sa 8^e Plénière (décembre 2012), le Comité de la Convention sur la Cybercriminalité (T-CY) a décidé de publier des Notes d'orientation visant à faciliter l'usage et la mise en œuvre effectives de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des développements du droit, des politiques et des techniques⁵⁰.

Bien qu'elles ne soient pas contraignantes, les Notes d'orientation reflètent une analyse de l'application de la Convention partagée par toutes ses Parties.

La présente Note⁵¹ traite la question des injonctions de produire relatives à des informations sur les abonnés visées à l'article 18, à savoir dans des situations où :

- une personne à qui il est fait injonction de produire des données informatiques spécifiées est présente sur le territoire d'un État Partie (Article 18.1.a);⁵²
- un fournisseur de services à qui il est fait injonction de produire des informations sur un abonné propose un service sur le territoire de l'État Partie sans forcément être situé sur le territoire en question (Article 18.1.b).

Il est pertinent de publier une Note d'orientation sur ces aspects de l'Article 18, étant donné :

- que les informations sur les abonnés sont le plus souvent recherchées dans des enquêtes pénales ;
- que l'article 18 a une compétence nationale ;
- que, du fait de l'essor du « cloud computing » et du stockage de données à distance, les autorités compétentes cherchant à accéder à des données informatiques spécifiées - en particulier à des informations relatives à l'abonné - pour mener des enquêtes pénales et des poursuites, se sont heurtées à un certain nombre de difficultés ;

49. Adoptée par le T-CY suite à la 16^{ième} plénière par procédure écrite (28 février 2017)

50. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

51. Cette Note d'orientation s'appuie sur les travaux du Groupe sur les Preuves dans le Cloud.

52. Il est important de rappeler que l'article 18.1.a de la Convention de Budapest n'est pas limité aux seules informations relatives aux abonnés, mais qu'il concerne tout type de données informatiques spécifiées. En revanche, la présente Note d'orientation ne traite que la seule production d'informations concernant les abonnés.

- qu’actuellement, les pratiques et les procédures, ainsi que les conditions et les sauvegardes en matière d’accès à des informations concernant les abonnés varient considérablement d’un État Partie de la Convention à l’autre ;
- qu’il est nécessaire de traiter les problèmes qui se posent en matière de vie privée et de protection des données à caractère personnel, pour ce qui est du fondement juridique de la juridiction relative aux services offerts sur le territoire d’un État partie sans que le fournisseur de services soit établi sur ce territoire, ainsi qu’en ce qui concerne l’accès à des données stockées dans des juridictions étrangères ou en des lieux inconnus ou multiples « dans le cloud » ;

La notification et la force exécutoire des injonctions de produire nationales à l’encontre de fournisseurs établis hors du territoire d’un Etat Partie posent d’autres problèmes qui ne peuvent être traités dans le cadre d’une note d’orientation. Les Etats Parties peuvent demander les informations relatives aux abonnés par le biais de l’entraide judiciaire.

La mesure visée à l’article 18 doit s’appliquer dans des enquêtes et procédures pénales spécifiques relevant du champ d’application de l’article 14 de la Convention de Budapest. Les injonctions doivent donc être délivrées dans des cas spécifiques en ce qui concerne des abonnés spécifiés.

Article 18 de la Convention de Budapest⁵³

Texte de la disposition

Article 18 – Injonction de produire

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

53. Voir l’annexe pour l’article 18 et les extraits *in extenso* du Rapport explicatif.

Extrait du Rapport explicatif:

173. En vertu du paragraphe 1(a), toute Partie doit veiller à ce que ses autorités répressives compétentes aient le pouvoir d'ordonner à une personne présente sur son territoire de communiquer des données électroniques spécifiées, stockées dans un système informatique ou un support de stockage, qui sont en possession ou sous le contrôle de cette personne. L'expression «en possession ou sous le contrôle» fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé en possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la partie ayant ordonné leur communication (par exemple, sous réserve des privilèges applicables, toute personne qui reçoit l'injonction de produire des informations stockées sur son compte au moyen d'un service de stockage en ligne à distance, droit produire ces informations). Par ailleurs, la simple possibilité technique d'accéder à des données stockées à distance (par exemple, la possibilité, pour un utilisateur, d'accéder, par une liaison du réseau, à des données stockées à distance qui ne sont pas sous son contrôle légitime) ne constitue pas nécessairement un «contrôle» au sens de la présente disposition. Dans certains États, la notion juridique de «possession» recouvre la possession matérielle et de droit de manière assez large pour satisfaire à cette exigence de «possession ou de contrôle».

En vertu du paragraphe 1(b), toute Partie doit aussi instaurer le pouvoir d'ordonner à un fournisseur de services offrant ceux-ci sur son territoire, de «communiquer les données relatives à l'abonné qui sont en possession ou sous le contrôle de ce fournisseur de services». De même qu'au paragraphe 1(a), l'expression «en possession ou sous le contrôle» fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement ou à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société). L'expression «qui se rapportent à ces services» signifie que le pouvoir en question doit servir à obtenir des informations relatives à l'abonné qui se rapportent à des services proposés sur le territoire de la Partie à l'origine de l'injonction⁵⁴.

2.2. Que recouvre l'expression « données relatives aux abonnés » ?

L'expression « données relatives aux abonnés » est définie à l'article 18.3 de la Convention de Budapest :

- 3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, contenue sous forme de données informatiques ou

54. Paragraphe 173 du Rapport explicatif.

sous toute autre forme, détenue par un fournisseur de services et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

- a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
- b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ;
- c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service.

Paragraphe 177 du rapport explicatif indique également :

177. L'expression « informations relatives aux abonnés » est définie au paragraphe 3. En principe, elle désigne toute information détenue par l'administration d'un fournisseur de services et qui se rapporte à un abonné à ses services. Les données relatives aux abonnés peuvent être contenues sous forme de données informatiques ou sous toute autre forme, telle que des documents-papier. Comme les informations relatives aux abonnés ne se présentent pas toutes sous la forme de données informatiques, une disposition spéciale a été insérée dans l'article pour tenir compte de ce type d'informations. Le terme d'« abonné » vise à englober de nombreuses catégories de clients des fournisseurs de services : personne ayant payé un abonnement, client qui paie au fur et à mesure les services qu'il utilise, personne bénéficiant de services gratuits. Sont aussi incluses les informations concernant les personnes habilitées à utiliser le compte de l'abonné.

L'obtention de données relatives aux abonnés peut constituer une ingérence moins contraignante à l'égard des droits individuels que l'obtention de données relatives au trafic ou au contenu.

Qu'est-ce qu'un « fournisseur de services » ?

La Convention de Budapest sur la cybercriminalité prévoit une notion large du « fournisseur de services », qui est défini à l'article 1.c de la Convention de Budapest.

Aux fins de la présente Convention, l'expression :

- c. « fournisseur de services » *désigne :*

- i. toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique;
- ii. toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

L'article 18.1.b s'applique pour tout fournisseur de services offrant des services sur le territoire de la Partie⁵⁵.

Interprétation par le T-CY de l'article 18 de la Convention de Budapest en ce qui concerne les données relatives aux abonnés

Portée de l'article 18.1.a

- La portée est large: une « personne » (notion qui peut englober celle de « fournisseur de services ») qui est présente sur le territoire de la Partie.
- Pour ce qui est des données informatiques, la portée est large mais n'est pas indéfinie: toutes données informatiques « spécifiées » (ce qui entraîne que l'article 18.1.a n'est pas limité aux « données relatives aux abonnés » et couvre tout type de données informatiques).
- Les données informatiques spécifiées sont en possession de cette personne ou si la personne n'en a pas la possession physique, elle contrôle librement les données informatiques transmises dans le cadre de l'article 18.1.a. depuis le territoire de l'Etat Partie.
- Les données informatiques spécifiées sont stockées dans un système informatique ou un moyen de stockage informatique.
- L'injonction de produire est émise et exécutable par les autorités compétentes dans la l'Etat Partie dans lequel l'injonction est demandée/ accordée.

Portée de l'article 18.1.b

La portée de l'article 18.1.b est plus étroite que celle de l'article 18.1.a. L'alinéa b:

- est limité au « fournisseur de services »⁵⁶;

55. Les instruments de l'Union européenne font la distinction entre fournisseurs de services de communication électroniques et fournisseurs de services dans la société de l'Internet. La notion de « fournisseur de services » visée à l'article 1.c de la Convention de Budapest recouvre ces deux aspects.

56. Le concept de « personne » est plus large que celui de « fournisseur de services », même si un « fournisseur de services » peut être une « personne ».

- le fournisseur de services destinataire de l'injonction n'est pas nécessairement présent sur le territoire mais offre ses services sur le territoire de l'Etat Partie ;
- est limité aux « données relatives aux abonnés » ;
- les données relatives aux abonnés sont liées à ces services et sont dans la possession ou le contrôle du fournisseur de service.

En revanche, contrairement à l'article 18.1.a. qui est limité dans son champs d'application « aux personnes présentes sur le territoire de l'Etat Partie, l'article 18.1.b est silencieux sur la question du lieu de situation du fournisseur de services. Les Parties pourraient mettre en œuvre la disposition dans des circonstances où le fournisseur de service offrant ses services sur le territoire de l'Etat Partie n'est ni juridiquement, ni physiquement, présent sur le territoire.

Compétence

L'article 18.1.b est limité aux circonstances où l'autorité de justice pénale délivrant l'injonction de produire est compétente pour l'infraction.

Cela peut concerner les situations où l'abonné est ou était résident ou présent sur le territoire lors de la commission de l'infraction.

La présente interprétation de l'article 18 ne préjuge pas de compétences plus larges ou supplémentaires en vertu du droit interne des Parties.

L'accord à la présente Note d'orientation n'implique ni le consentement à la notification ou la force exécutoire extraterritoriale d'une ordonnance de production nationale délivrée par un autre État ni de créer de nouvelles obligations ou relations entre les Etats Parties.

Quelles sont les caractéristiques d'une « injonction de produire » ?

Une « injonction de produire » au sens de l'article 18 est une mesure nationale qui doit être prise selon le droit pénal interne. Elle est limitée par la compétence d'adjudication et d'exécution de la Partie dans laquelle l'injonction est délivrée.

Les injections de produire relevant de l'article 18 portent « sur des données informatiques ou des informations relatives à l'abonné qui sont en la possession ou sous le contrôle d'une personne ou d'un fournisseur

de services. La mesure n'est applicable que pour autant que la personne ou le fournisseur de services conserve ces données ou ces informations. Certains fournisseurs de services, par exemple, ne gardent pas trace des usagers de leurs services.»⁵⁷

Le rapport explicatif⁵⁸ de la Convention de Budapest mentionne les injonctions de reproduire comme une mesure souple, moins contraignante que la perquisition ou la saisie ou encore d'autres pouvoirs coercitifs :

«l'instauration d'un tel mécanisme procédural sera aussi utile pour les tiers gardiens des données qui, tels les fournisseurs d'accès Internet, sont souvent disposés à collaborer avec les services de lutte contre la criminalité sur une base volontaire en leur fournissant les données sous leur contrôle, mais préfèrent disposer d'une base juridique appropriée pour apporter cette aide, les déchargeant de toute responsabilité contractuelle ou autre.»

Quel effet produit la localisation des données ?

Le fait que les informations relatives aux abonnés soient stockées dans une autre juridiction ne fait pas obstacle à l'application de l'article 18 de la Convention de Budapest. Le Rapport explicatif précise :

- concernant l'article 18.1.a, que « l'expression « en possession ou sous le contrôle » fait référence à la possession matérielle des données concernées sur le territoire de la Partie qui a ordonné leur communication, et à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut contrôler librement la production de ces données depuis le territoire de la Partie ayant ordonné leur communication.»⁵⁹ ;
- concernant l'article 18.1.b, que « l'expression « en possession ou sous le contrôle » fait référence à des données relatives à l'abonné que le fournisseur de services possède matériellement et à des données relatives à l'abonné stockées à distance qui sont sous le contrôle du fournisseur de services (ces données peuvent par exemple être stockées dans une unité de stockage à distance fournie par une autre société) »⁶⁰.

57. Paragraphe 172 du Rapport explicatif.

58. Paragraphe 171 du Rapport explicatif.

59. Paragraphe 173 du Rapport explicatif. Une « personne » au sens de l'article 18.1.a de la Convention de Budapest peut être une personne physique ou une personne morale, notamment un fournisseur de services.

60. Paragraphe 173 du Rapport explicatif.

En ce qui concerne l'article 18.1.b, une situation possible peut être celle où un fournisseur de services a son siège dans une juridiction mais stocke les données dans une autre juridiction. Des données peuvent être répliquées dans plusieurs juridictions ou se déplacer entre plusieurs juridictions à la discrétion du fournisseur de services sans information ni contrôle de l'abonné. Les régimes juridiques admettent de plus en plus, tant dans la sphère du droit pénal qu'en matière de protection de la vie privée et des données, que la localisation des données n'est pas le facteur déterminant pour établir la compétence juridictionnelle.

Que recouvre la notion de « offrant des prestations sur le territoire d'une Partie » ?

L'essor du « Cloud computing » a amené à s'interroger sur le point de savoir quand un fournisseur de services est considéré comme offrant ses prestations sur le territoire de la Partie et étant par là-même tenu d'obéir à une injonction nationale de produire des données relatives à un abonné. Cette question a fait l'objet d'une série d'interprétation par les tribunaux dans diverses juridictions, dans des affaires civiles comme pénales.

En ce qui concerne l'article 18.1.b, un fournisseur de services « offre un service sur le territoire de la partie » lorsque :

- le fournisseur de services permet à des personnes sur le territoire de la Partie de s'abonner à ses services⁶¹ (et ne bloque pas, par exemple, l'accès à ce type de services) ;

et

- le fournisseur de service a établi un lien réel et substantiel à un Etat Partie. Les facteurs pertinents peuvent inclure la mesure dans laquelle un fournisseur de service oriente ses activités vers ces abonnés (par exemple, en faisant localement de la publicité ou en faisant de la publicité dans la langue du territoire de la Partie), ou utilise les informations relatives aux abonnés (ou les données de trafic associées) dans le cours de ses activités, ou interagit avec des abonnés dans l'Etat Partie et peut en d'autre terme être considéré comme établi sur le territoire de l'Etat Partie.

61. Veuillez noter le Paragraphe 183 Rapport explicatif : « La mention d'un « contrat ou arrangement de service » s'entend au sens très large de toute type de relation sur la base duquel un abonné utilise les services d'un fournisseur ».

Le simple fait qu'un fournisseur de service utilise un nom de domaine ou une adresse mail électronique connecté à un pays spécifique ne crée pas une présomption que son lieu d'établissement soit dans ce pays. C'est pourquoi, la condition qui exige que les données relatives aux abonnés soient en lien avec des services offerts par un fournisseur sur le territoire de l'Etat Partie, peut être considérée comme remplie même si ces services sont fournis via un domaine national de premier niveau faisant référence à une autre juridiction.

Considérations générales et sauvegardes

Les Parties à la Convention sont tenues de former une communauté de confiance qui respecte l'article 15 de la Convention de Budapest.

Article 15 – Conditions et sauvegardes

1 - Chaque 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, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 - Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question. 3 - Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Application de l'article 18 en ce qui concerne les données relatives aux abonnés

La production de données relatives aux abonnés en vertu de l'article 18 de la Convention de Budapest peut donc être ordonnée si les critères suivants sont remplis dans une enquête pénale spécifique et pour des abonnés spécifiés :

SI		
l'autorité de justice pénale est compétente pour l'infraction ;		
ET SI		
le fournisseur de services possède ou contrôle les données relatives à l'abonné ;		
ET SI		
Article 18.1.a	OU	Article 18.1.b
Le fournisseur de services est présent sur le territoire de la Partie.		Un Etat Partie considère qu'un fournisseur de service « offre ses services sur le territoire de la Partie », lorsque, par exemple : – le fournisseur de services permet à des personnes sur le territoire de la Partie de s'abonner à ses services (et ne bloque pas par exemple l'accès à ce type de services) ; ET – le fournisseur de service a établi un lien réel et substantiel à un Etat Partie. Les facteurs pertinents peuvent inclure : dans quelle mesure un fournisseur de service oriente ses activités vers ces abonnés (par exemple, en faisant localement de la publicité ou en faisant de la publicité dans la langue du territoire de la Partie), ou utilise les informations relatives aux abonnés (ou les données de trafic associées) dans le cours de ses activités, ou interagit avec des abonnés dans l'Etat Partie et peut en d'autre terme être considéré comme établi sur le territoire de l'Etat Partie.
ET SI		
		– les données relatives aux abonnés devant être produites concernant les services d'un fournisseur offerts sur le territoire de l'Etat Partie.

Déclaration du T-CY

Le T-CY s'accorde à dire que les positions présentées ci-dessus constituent le socle commun sur lequel s'entendent les Parties en ce qui concerne la portée et les éléments de l'article 18 de la Convention de Budapest concernant la production de données relatives aux abonnés.

Note d'orientation sur le terrorisme⁶²

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies.⁶³

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente Note traite de la manière dont différents articles de la Convention s'appliquent au terrorisme.

Bon nombre de pays sont parties à de nombreux traités, et soumis aux Résolutions du Conseil de Sécurité des Nations Unies, qui exigent l'incrimination de différentes formes de terrorisme, de la facilitation du terrorisme, du soutien au terrorisme et des actes préparatoires au terrorisme.

Dans des affaires de terrorisme, les pays s'appuient souvent sur des infractions qui dérivent de ces traités visant des thèmes spécifiques, ainsi que sur des infractions supplémentaires incriminées en droit interne.

La Convention de Budapest n'est pas un traité s'appliquant spécifiquement au terrorisme. Toutefois, les infractions matérielles visées par la Convention peuvent être transposées aux actes de terrorisme, pour faciliter le terrorisme, pour soutenir le terrorisme – y compris financièrement – ou aux actes préparatoires au terrorisme.

En outre, les outils procéduraux et d'entraide judiciaire internationales prévus dans la Convention sont applicables aux enquêtes et poursuites pour faits de terrorisme et connexes à ces infractions.

La portée et les limites sont définies par les articles par les articles 14.2 et 25.1 de la Convention de Budapest :

Article 14 2

2. Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

- a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

62. Adoptée lors de la 16ème réunion plénière du T-CY (14-15 novembre 2016)

63. Voir le mandat du T-CY (Article 46 Convention de Budapest).

- b à toutes les autres infractions pénales commises au moyen d'un système informatique; et
- c à la collecte des preuves électroniques de toute infraction pénale.

Article 25.1

« Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. »

Le lecteur peut également se référer aux articles 23 et 27.1 de la Convention de Budapest ainsi que les Notes d'orientation, telles que celles sur les attaques visant des infrastructures d'information critiques ou celle sur les attaques par déni de service et déni de service distribué.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (ETS 185)

Dispositions procédurales

Les pouvoirs procéduraux visés par la Convention à ses articles 14 à 21 peuvent être utilisés dans une enquête ou procédure pénale spécifique relevant de tout type d'affaire, comme le prévoit l'article 14.

De fait, les mesures procédurales spécifiques peuvent être très utiles, pour exemple dans une affaire de terrorisme, si un système informatique a été utilisé pour commettre ou faciliter une infraction ou si les preuves de l'infraction sont stockées sous forme électronique, ou encore si un suspect peut être identifié grâce aux informations relatives à l'abonné, y compris pour ce qui est d'une adresse IP (Internet Protocol). Ainsi, dans des affaires de terrorisme, les parties peuvent recourir à la conservation accélérée, aux injonctions de produire, aux ordonnances de perquisition et de saisie ainsi qu'à d'autres outils pour recueillir les preuves dans des enquêtes et poursuites en matière de terrorisme ou d'affaires connexes dans le cadre du champs exposé ci au-dessus.

Dispositions relatives à l'entraide judiciaire internationale

Les pouvoirs en matière de coopération internationale (articles 23 à 35) sont d'une portée similaire.

Ainsi, les Parties doivent assurer la conservation accélérée, délivrer des injonctions de produire, des ordonnances de perquisition et de saisie ainsi qu'utiliser

d'autres outils ainsi que d'autres dispositions de coopération internationale disponibles pour coopérer avec d'autres Parties dans des enquêtes et poursuites en matière de terrorisme ou d'affaires connexes dans le cadre du champs exposé ci au-dessus.

Dispositions de droit pénal matériel

Enfin, comme indiqué plus haut, les terroristes et groupes terroristes peuvent perpétrer des actes incriminés par la Convention pour parvenir à leurs fins.

Articles pertinents	Exemples
Article 2 – Accès illégal	Il peut y avoir accès illégal à un système informatique pour obtenir des informations permettant l'identification personnelle (par exemple, informations concernant des employés publics qui permettront d'en faire la cible d'une attaque).
Article 3 – Interception illégale	Des transmissions non-publiques de données informatiques vers, depuis ou dans un système informatique peuvent être interceptées illégalement pour obtenir des informations concernant le lieu où se trouve une personne (afin de la cibler).
Article 4 – Atteinte à l'intégrité des données	Des données informatiques peuvent être endommagées, effacées, détériorées, altérées ou supprimées (ainsi, les enregistrements médicaux d'un hôpital peuvent être altérés et devenir dangereux du fait qu'ils sont incorrects, ou encore l'interférence avec un système de contrôle de trafic aérien peut avoir des conséquences pour la sûreté des vols).
Article 5 – Atteinte à l'intégrité du système	Le fonctionnement d'un système informatique peut être entravé à des fins terroristes (par exemple, entrave au bon fonctionnement du système qui stocke les enregistrements des opérations boursières, ce qui peut rendre ces dernières non fiables, ou encore entrave au fonctionnement d'infrastructures critiques).
Article 6 – Abus de dispositifs	La vente, l'achat en vue de l'utilisation, l'importation, la distribution ou autre forme de mise à disposition de mots de passes, codes d'accès informatiques ou données similaires permettant l'accès de systèmes informatiques peuvent faciliter une attaque terroriste (par exemple, permettre d'endommager le réseau de distribution d'électricité d'un pays).

Articles pertinents	Exemples
Article 7 – Falsification informatique	Des données informatiques (par exemple celles utilisées dans les passeports électroniques) peuvent être ajoutées, altérées, effacées ou supprimées, avec pour conséquence que des données non authentiques sont prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.
Article 8 – Fraude informatique	Des données informatiques peuvent être ajoutées, altérées, effacées ou supprimées, et/ou le fonctionnement d'un système informatique altéré, avec pour résultat que des victimes perdent des biens ou avoirs (par exemple, une attaque contre le système bancaire d'un pays peut entraîner la perte d'avoirs pour un certain nombre de victimes).
Article 11 – Tentative et complicité	Les infractions spécifiées dans le traité peuvent donner lieu à tentative ou complicité à des fins terroristes.
Article 12 – Responsabilité des personnes morales	Les infractions couvertes par les articles 2-12 de la Convention dans la promotion du terrorisme peuvent être réalisées par des personnes morales qui seraient tenues comme responsable sous l'article 12.
Article 13 – Sanctions	Les infractions couvertes par la Convention peuvent constituer une menace à l'égard des individus et de la société, en particulier lorsqu'elles visent des systèmes critiques au quotidien – par exemple, les systèmes bancaires ou les hôpitaux. Les conséquences seront variables dans chaque pays en fonction du degré d'interconnectivité et de la dépendance à de tels systèmes. Une Partie peut prévoir dans son droit interne une sanction par trop clémentine pour les actes liés au terrorisme en lien avec les articles 2 à 11, ou encore ne pas prévoir de circonstances aggravantes en cas de tentative ou de complicité. Des Parties pourraient avoir à envisager de modifier leur droit interne. En vertu de l'article 13 de la Convention, les Parties doivent veiller à ce que les infractions pénales liées à de tels actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté. »

Articles pertinents	Exemples
	Les Parties peuvent aussi envisager de faire jouer des circonstances aggravantes, par exemple si de tels actes affectent un nombre significatif de systèmes ou causent des dégâts considérables, notamment des morts ou des blessés, ou endommagent des infrastructures critiques.

D'autres infractions couvertes par la Convention mais qui ne sont pas mentionnées spécifiquement ci-dessus, notamment la production de matériel lié à l'exploitation des enfants ou le trafic de piratage de propriété intellectuelle, peuvent aussi être commises en lien avec le terrorisme.

Pour les Parties à la Convention de Budapest qui sont Parties au Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE 189)⁶⁴, deux articles de ce dernier sont pertinents puisque ces phénomènes peuvent contribuer à la radicalisation et à l'extrémisme violent menant au terrorisme: l'article 4 couvrant les menaces avec une motivation raciste ou xénophobe et l'article 6 couvrant la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité.

Déclaration du T-CY

Le T-CY convient que les infractions matérielles visées par la Convention peuvent constituer des actes de terrorisme tel que défini dans le droit applicable.

Plus généralement, les infractions matérielles visées par la Convention peuvent être commises pour faciliter le terrorisme, le soutenir – y compris financièrement – ou le préparer.

Les outils procéduraux et d'entraide judiciaire internationale prévus dans la Convention peuvent servir aux enquêtes sur des faits de terrorisme, leur facilitation, le soutien ou des actes préparatoires au terrorisme.

64. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

Note d'orientation sur les aspects de l'ingérence électorale au moyen de systèmes informatiques couverts par la Convention de Budapest⁶⁵

Introduction

Lors de sa 8^e réunion plénière (décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies⁶⁶.

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

L'ingérence dans les élections par des cyberactivités malveillantes ciblant les ordinateurs et les données utilisées lors des élections et des campagnes électorales compromet la tenue d'élections libres, équitables et régulières et sape la confiance dans la démocratie. Les opérations de désinformation, telles qu'elles sont vécues en particulier depuis 2016, peuvent recourir à de telles pratiques et avoir le même effet. Les procédures électorales nationales doivent être adaptées aux réalités de la société de l'information et les systèmes informatiques utilisés pour les élections et les campagnes électorales doivent être rendus plus sûrs.

Dans ce contexte, il faut redoubler d'efforts pour poursuivre ces ingérences lorsqu'elles constituent une infraction pénale : une réponse efficace de la justice pénale peut dissuader de se livrer à une ingérence électorale et rassurer l'électorat quant à l'utilisation des technologies de l'information et de la communication dans les élections.

La présente note traite de la manière dont les articles de la Convention peuvent s'appliquer aux aspects de l'ingérence électorale au moyen de systèmes informatiques.

Les infractions matérielles définies dans la Convention peuvent être commises en tant qu'actes d'ingérence électorale ou en tant qu'actes préparatoires facilitant cette ingérence.

65. Adoptée par le T-CY lors de sa 21^e réunion plénière (8 juillet 2019).

66. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

En outre, les outils nationaux de procédure et d'entraide judiciaire internationale de la Convention sont disponibles aux fins d'enquêtes et de poursuites liées à l'ingérence électorale. La portée et les limites des pouvoirs procéduraux et des outils de coopération internationale sont définies par les articles 14.2 et 25.1 de la Convention de Budapest :

Article 14.2

2. Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
 - a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
 - b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et
 - c à la collecte des preuves électroniques de toute infraction pénale.

Article 25.1

Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

Les pouvoirs et procédures énoncés dans la Convention sont soumis aux conditions et sauvegardes prévues à l'article 15.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STE 185)

Dispositions procédurales

Les pouvoirs et procédures énoncés dans la Convention (articles 14 à 21) peuvent être appliqués dans le cadre d'une enquête ou d'une procédure pénale spécifique dans tout type d'ingérence électorale, comme prévu à l'article 14.

Les mesures procédurales spécifiques peuvent être très utiles dans les enquêtes pénales pour ingérence électorale. Par exemple, dans ce type d'affaire, un système informatique peut être utilisé pour commettre ou faciliter une infraction, la preuve de cette infraction peut être stockée sous forme électronique, ou un suspect peut être identifiable grâce aux renseignements sur l'abonné, y compris une adresse IP. De même, le financement politique illégal peut être traçable par le biais de courriels préservés, les communications vocales entre conspirateurs peuvent être saisies à la suite d'une interception dûment autorisée, et le mauvais usage des données peut être illustré par des pistes électroniques.

Ainsi, dans les enquêtes pénales portant sur des infractions liées à l'ingérence électorale, les Parties peuvent faire usage de leur pouvoir d'ordonner la conservation rapide des données informatiques stockées et de leurs pouvoirs d'injonction de produire, de perquisition et de saisie de données informatiques stockées, ainsi que d'autres outils permettant la collecte de preuves électroniques aux fins d'investigations et de poursuite de telles infractions.

Dispositions relatives à l'entraide judiciaire internationale

Les pouvoirs prévus par la Convention en matière de coopération internationale (articles 23 à 35) sont d'une portée similaire et peuvent aider les Parties dans les enquêtes sur les ingérences électorales.

Ainsi, les Parties mettent en œuvre les actions requises – conservation rapide des données informatiques stockées, injonction de produire, perquisition et saisie de données informatiques stockées –, ainsi que d'autres dispositifs de coopération internationale.

Dispositions de droit pénal matériel

Enfin, comme on l'a vu plus haut, l'ingérence électorale peut concerner les types de comportement suivants (lorsqu'ils sont commis sans avoir de fondement légal), érigés en infraction pénale par la Convention sur la cybercriminalité. Le T-CY souligne que les agissements cités ne sont que de simples exemples – l'ingérence électorale est en effet un phénomène qui prend de l'ampleur et peut revêtir des formes multiples, non énumérées ci-dessous. Le comité estime néanmoins que la Convention sur la cybercriminalité est suffisamment souple pour y remédier.

Articles pertinents	Exemples
Article 2 – Accès illégal	Un système informatique peut être utilisé illégalement pour obtenir des informations sensibles ou confidentielles relatives à des candidats, des campagnes, des partis politiques ou des électeurs.
Article 3 – Interception illégale	Lors de transmissions non publiques à destination, en provenance ou à l'intérieur d'un système informatique, des données informatiques peuvent être interceptées illégalement pour obtenir des informations sensibles ou confidentielles relatives à des candidats, des campagnes, des partis politiques ou des électeurs.

Article 4 – Atteinte à l'intégrité des données	Les données informatiques peuvent être endommagées, effacées, détériorées, altérées ou supprimées pour modifier des sites internet, altérer les listes électorales ou falsifier les résultats des élections, par exemple en manipulant des machines à voter.
Article 5 – Atteinte à l'intégrité du système	Le fonctionnement des systèmes informatiques utilisés lors d'élections ou de campagnes électorales peut être entravé pour interférer avec les messages de la campagne, entraver l'inscription des électeurs, désactiver les dispositifs de vote ou empêcher le décompte des voix par des attaques en déni de service, des logiciels malveillants ou d'autres moyens.
Article 6 – Abus de dispositifs	La vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à un système informatique peuvent faciliter l'ingérence électorale (par exemple vol de données sensibles de candidats politiques, de partis ou de campagnes).
Article 7 – Falsification informatique	Des données informatiques (par exemple les données des listes électorales) peuvent être introduites, altérées, effacées ou supprimées, de sorte que des données non authentiques sont prises en compte ou utilisées à des fins légales comme si elles étaient authentiques. Par exemple, certains pays exigent que les campagnes électorales fassent l'objet d'une déclaration de situation financière publique. La falsification de données informatiques pourrait donner l'impression de divulgations inexactes ou cacher des sources douteuses de fonds de campagne.
Article 11 – Tentative et complicité	La tentative de commettre l'une quelconque des infractions définies dans le traité, ou tout acte de complicité par aide ou assistance, en vue d'exercer une ingérence électorale.
Article 12 – Responsabilité des personnes morales	L'une quelconque des infractions visées aux articles 2 à 11 de la Convention peut être commise, en vue d'exercer une ingérence électorale, par des personnes morales qui pourraient être tenues pour responsables en vertu de l'article 12.

Article 13 – Sanctions et mesures	Les infractions visées par la Convention peuvent constituer une menace pour les individus et la société, en particulier lorsque ces infractions sont dirigées contre les fondements de la vie politique, comme les élections. Les actes criminels et leurs effets peuvent différer d'un pays à l'autre, mais l'ingérence électorale peut miner la confiance dans les processus démocratiques, modifier le résultat d'une élection, obliger à organiser un second scrutin avec les coûts et les éventuels troubles que cela comporte, voire provoquer des violences physiques entre les partisans de la tenue d'élections et d'autres citoyens. Une Partie peut prévoir dans son droit interne une sanction trop clémente pour des actes visés aux articles 2 à 11 commis dans le cadre d'élections, et ne pas autoriser la prise en compte de circonstances aggravantes ou des notions de tentative et de complicité. Dans cette hypothèse, elle devrait envisager de modifier les dispositions pertinentes. Les Parties doivent veiller, conformément à l'article 13, à ce que les infractions pénales liées à de tels actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Les Parties peuvent également envisager des circonstances aggravantes, par exemple si de tels actes affectent de manière significative une élection ou causent des décès ou des dommages corporels ou des dégâts matériels importants.
---	---

Déclaration du T-CY

Le T-CY convient que les infractions matérielles définies dans la Convention sont également susceptibles de constituer des actes d'ingérence électorale tels que définis par le droit applicable, c'est-à-dire des agissements portant atteinte à la tenue d'élections libres, équitables et régulières.

Les infractions matérielles définies dans la Convention peuvent être commises dans le but de faciliter, participer à, ou préparer des actes d'ingérence électorale.

Les outils de procédure et d'entraide judiciaire de la Convention peuvent être utilisés pour enquêter sur l'ingérence électorale, sa facilitation et la participation à celle-ci, ou sur les actes préparatoires à ladite ingérence.

Note d'orientation sur les aspects des logiciels rançonneurs couverts par la Convention de Budapest⁶⁷

Introduction

À sa 8^e session plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en œuvre effectives de la Convention sur la cybercriminalité, notamment à la lumière des faits nouveaux apparus dans les domaines juridique, politique et technique⁶⁸.

Ces notes d'orientation reflètent l'analyse de l'application de la Convention de Budapest partagée par toutes les Parties.

Depuis des dizaines d'années, des délinquants commettent des délits de cybercriminalité sous diverses formes dans le but de rançonner des organisations et des particuliers. Ainsi, le vol de données à caractère personnel ou d'autres informations sensibles suivi de la menace de leur divulgation publique afin d'obtenir le versement d'une rançon est un délit toujours largement répandu. Mais on a vu apparaître, ces dix dernières années, des logiciels rançonneurs et des infractions associées de formes plus complexes. On citera, par exemple, le cryptage de données ou systèmes informatiques destiné à verrouiller l'accès des utilisateurs, suivi de demandes de rançons en échange (de la promesse) du rétablissement des accès. Les auteurs de ce type d'infraction peuvent aussi menacer leurs victimes de publier des données sensibles ou à caractère personnel afin de leur soutirer de l'argent plus facilement.

Ces infractions par logiciels rançonneurs sont possibles parce que la technologie permet :

- un cryptage fort des données ou systèmes informatiques des victimes ;
- l'envoi de demandes de rançon et d'outils de décryptage au moyen de systèmes de communication difficiles à localiser ;
- le versement de rançons par des moyens difficiles à retracer, notamment via des monnaies virtuelles, qui sont plus faciles à masquer que les monnaies fiduciaires.

Les attaques «WannaCry» et «NotPetya» de 2016/2017, qui visaient des ordinateurs, ont suscité une grande attention dans le monde entier. Depuis la

67. Adoptée par le T-CY lors de sa 27^e réunion plénière (29-30 novembre 2022).

68. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

pandémie de covid-19 qui a démarré en 2020, les sociétés sont beaucoup plus dépendantes des technologies de l'information et de la communication, ce qui accroît les possibilités d'exploitation à des fins criminelles. Ce phénomène a contribué à une forte augmentation des infractions par logiciels rançonneurs. Certaines attaques contre des systèmes informatiques de centres hospitaliers seraient ainsi à l'origine de décès de patients. En outre, en avril 2022, des infractions de ce type menées contre des infrastructures critiques au Costa Rica ont obligé le pays à déclarer l'état d'urgence nationale. L'utilisation de logiciels rançonneurs est aujourd'hui considérée comme une forme grave de cybercriminalité qui porte atteinte aux intérêts essentiels des individus, des entreprises, des sociétés et des États.

Le T-CY a donc décidé, lors de sa 26^e session plénière (10-11 mai 2022), de rédiger une note d'orientation montrant comment les infractions par logiciels rançonneurs, sous leurs divers aspects, sont incriminées au titre des dispositions de droit pénal matériel de la Convention sur la cybercriminalité et comment les dispositions et pouvoirs de procédure en matière de coopération internationale de ce traité peuvent être utilisés dans les enquêtes, les poursuites et la coopération dans la lutte contre ces infractions.

La présente note d'orientation fait également référence au [Deuxième Protocole additionnel à la Convention sur la cybercriminalité \(STCE n° 224\)](#), qui apportera aux Parties à ce Protocole, une fois en vigueur, de nouveaux outils pour le « renforcement de la coopération et de la divulgation de preuves électroniques ».

Les précédentes notes d'orientation du T-CY relatives aux [logiciels malveillants](#), aux [botnets](#), aux [fraudes par usurpation d'identité](#) et aux [attaques contre les infrastructures critiques](#) sont aussi applicables aux infractions par logiciels rançonneurs.

Les infractions par logiciels rançonneurs

Un logiciel rançonneur est un type de logiciel malveillant consistant à bloquer l'accès d'un utilisateur à ses données ou systèmes informatiques au moyen d'un cryptage de ces données ou systèmes. L'utilisateur visé est invité à payer une rançon en échange (de la promesse) du rétablissement de l'accès à ses données ou systèmes.

Le plus souvent, les infractions par logiciels rançonneurs supposent :

1. Des actions préparatoires, notamment :

- la production, la vente, l’obtention ou autres formes de mise à disposition d’un logiciel rançonneur, c’est-à-dire un « dispositif » au sens de l’article 6 de la Convention sur la cybercriminalité ;
- la production, la vente, l’obtention ou autres formes de mise à disposition d’autres dispositifs, au sens de l’article 6, qui sont utilisés pour préparer des infractions par logiciels rançonneurs, tels que des logiciels malveillants permettant d’obtenir un accès non autorisé aux systèmes ciblés ou des botnets destinés à diffuser des logiciels rançonneurs ;
- l’obtention de listes de distribution ou d’autres informations importantes concernant les cibles. Certaines de ces actions préparatoires peuvent elles-mêmes constituer des infractions ou être considérées comme une aide ou une incitation à commettre des infractions par logiciels rançonneurs, comme l’exfiltration de bases de données au moyen d’enregistreurs de frappe, l’utilisation de botnets ou l’usurpation d’identité⁶⁹.

2. La diffusion ou l’installation de logiciels rançonneurs, notamment :

- via des e-mails dont les pièces jointes contiennent le logiciel malveillant ou en envoyant aux utilisateurs d’applications de messagerie des liens intégrés dans des messages. Pour inciter davantage les utilisateurs à accéder à ces pièces jointes ou à ces liens – et donc à installer le logiciel malveillant –, les délinquants ont parfois recours à l’ingénierie sociale ou à d’autres techniques d’usurpation d’identité ;
- en accédant à distance à un système informatique.

3. Le cryptage du système informatique, de certaines de ses parties ou de données au moyen du logiciel rançonneur, empêchant ainsi l’utilisateur d’accéder aux données ou au système ou de les utiliser.

4. La demande, l’obtention et le transfert de la rançon, notamment :

- en demandant la rançon en échange (de la promesse) du rétablissement de l’accès aux données et/ou au système, ce qui s’analyse en une extorsion ou un chantage, mais aussi éventuellement en d’autres infractions ;
- la communication entre l’auteur de l’infraction et la personne prise pour cible par des moyens de communication difficiles à retracer, notamment l’utilisation de TOR. Les outils de décryptage peuvent également être communiqués de cette manière ;

69. Voir les [notes d’orientation \(coe.int\)](#) correspondantes.

- en obtenant la rançon d’une manière qui rende sa localisation difficile, généralement sous forme de cryptomonnaie, puis du blanchiment du produit de l’opération criminelle afin de dissimuler davantage l’identité de l’auteur et le produit.

Depuis 2021, le marché des logiciels rançonneurs est de plus en plus organisé et professionnel : il offre un modèle économique souvent appelé « logiciel rançonneur en tant que service » ou RaaS (*ransomware-as-a-service*), qui permet de commettre des infractions basées sur ce type de logiciel. Tirant parti de ce modèle économique, certains cybercriminels font appel à des services indépendants pour négocier les paiements et aider les victimes à effectuer les versements, certains services proposant un centre d’assistance 24/7 pour accélérer le paiement des rançons et aider à la restitution des systèmes ou données cryptés.

Dispositions pertinentes de la Convention sur la cybercriminalité (STE n° 185)

Incrimination des infractions par logiciels rançonneurs

En vertu de la Convention sur la cybercriminalité, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger certains actes en infractions pénales, conformément à son droit interne, lorsqu’ils sont commis intentionnellement et sans droit. Les articles suivants et les infractions correspondantes dans le droit interne des Parties appliquant la Convention seraient pertinents aux fins de l’ouverture d’enquêtes et de procédures pénales concernant les infractions par logiciels rançonneurs.

Articles pertinents	Exemples
Article 2 – Accès illégal	Les infractions par logiciels rançonneurs nécessitent un accès illégal à un système informatique de la victime et constituent donc une infraction pénale aux termes de l’article 2.
Article 3 – Interception illégale	Certaines variantes de logiciels rançonneurs ont la capacité d’intercepter des transmissions non publiques de données informatiques à destination, en provenance ou à l’intérieur d’un système informatique. L’obtention d’informations sur les cibles ou de clés d’accès peut aussi s’analyser en infraction d’interception illégale.

Article 4 – Atteinte à l'intégrité des données	Les logiciels rançonneurs sont spécialement conçus pour porter atteinte à l'intégrité de données informatiques; leur utilisation est donc une infraction pénale aux termes de l'article 4.
Article 5 – Atteinte à l'intégrité du système	Les logiciels rançonneurs peuvent être conçus pour porter atteinte au fonctionnement d'un système informatique; leur utilisation est donc une infraction pénale aux termes de l'article 5.
Article 6 – Abus de dispositifs	Un logiciel rançonneur est un logiciel malveillant, et donc un dispositif « principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ». Par conséquent, « la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition » d'un logiciel rançonneur est une infraction pénale aux termes de l'article 6.
Article 7 – Falsification informatique	Pour obtenir un accès illégal aux systèmes de la victime, les acteurs du logiciel rançonneur ont souvent recours au hameçonnage et à d'autres techniques d'ingénierie sociale, qui, dans certains cas, peuvent s'analyser en falsification informatique. Autrement dit, ils créent des données non authentiques dans le but qu'elles soient considérées ou traitées à des fins légales, comme le seraient des données authentiques.
Article 8 – Fraude informatique	Les infractions par logiciels rançonneurs causent un préjudice économique en portant atteinte à des données informatiques et/ou au fonctionnement d'un système informatique avec l'intention frauduleuse ou autrement malhonnête d'obtenir, sans droit, un avantage économique.
Article 11 – Tentative et complicité	Les infractions prévues dans le traité englobent la tentative ou la complicité commise en vue de perpétrer une infraction par logiciels rançonneurs. Différentes personnes peuvent être impliquées, par exemple, dans la production, l'obtention ou d'autres formes de mise à disposition d'un logiciel rançonneur, ou dans l'obtention d'informations sur les personnes prises pour cible.

Article 12 – Responsabilité des personnes morales	Les infractions par logiciels rançonneurs visées par les articles 2 à 11 de la Convention, telles que décrites ci-dessus, peuvent être commises par des personnes morales qui seraient responsables en vertu de l'article 12.
Article 13 – Sanctions	Les infractions par logiciels rançonneurs qui sont des infractions visées par la Convention peuvent faire peser une menace importante sur les personnes et la société, en particulier lorsqu'elles sont dirigées contre des infrastructures d'information critiques et entraînent un risque important pour la vie ou la sécurité de toute personne physique. Les Parties devraient donc veiller, conformément à l'article 13, à ce que les infractions pénales liées à ces actes « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Il s'agit notamment de veiller à ce que, dans le droit interne, les sanctions existantes soient adaptées à la menace que représentent les logiciels rançonneurs et prennent en considération l'ensemble des responsabilités pénales, y compris celles fondées sur la tentative de commettre un acte délictueux et la complicité en vue de la commission d'un tel acte. Les Parties peuvent également envisager des peines plus lourdes lorsqu'il y a des circonstances aggravantes, par exemple, si ces actes portent gravement atteinte au fonctionnement d'une infrastructure critique ou qu'ils provoquent la mort d'une personne physique ou lui causent des dommages corporels ou qu'ils sont à l'origine de dommages matériels importants.

Par conséquent, les infractions par logiciels rançonneurs peuvent comprendre des comportements devant être érigés en infractions pénales conformément aux articles 2 à 8 et à l'article 11 (tentative et complicité), ainsi que des comportements pouvant engager la responsabilité des personnes morales en vertu de l'article 12 de la Convention sur la cybercriminalité.

Les activités liées aux logiciels rançonneurs peuvent comprendre un large éventail d'autres infractions en vertu du droit pénal national.

Dispositions procédurales

En vertu de la Convention sur la cybercriminalité, «[c]haque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à» prendre certaines mesures procédurales pour enquêter sur les infractions visées aux articles 2 à 11 de la Convention et pour recueillir des preuves sous forme électronique (voir article 14 de la Convention). Ces mesures peuvent également être utilisées dans le cadre d'enquêtes et de procédures pénales liées à des infractions par logiciels rançonneurs.

Articles pertinents	Exemples
Article 14 – Portée d'application des mesures du droit de procédure	Les pouvoirs de procédure de la Convention (articles 16 à 21) peuvent être utilisés dans le cadre d'une enquête ou d'une procédure pénale particulière ayant trait non seulement aux infractions susmentionnées au titre de la Convention, mais également à la collecte de preuves sous forme électronique de toute autre infraction liée à un logiciel rançonneur telle que définie par le droit interne d'une Partie.
Article 15 – Conditions et sauvegardes	Ces conditions et sauvegardes s'appliquent également aux enquêtes et procédures pénales liées à des infractions par logiciels rançonneurs.
Article 16 – Conservation rapide de données informatiques stockées	Ce pouvoir peut être utilisé pour conserver rapidement des données informatiques stockées qui ont trait à des infractions par logiciels rançonneurs, notamment des données concernant la source ou le trajet de diffusion du logiciel rançonneur ou des communications relatives à la demande d'une rançon ou à la fourniture d'outils de décryptage, le cas échéant. Ce pouvoir peut également être utilisé pour ordonner la conservation d'autres données liées à des infractions par logiciels rançonneurs, telles que les communications entre les suspects ou les données stockées par les suspects et pouvant constituer des preuves de ces infractions.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic	Ce pouvoir peut être utilisé pour obtenir rapidement une quantité suffisante de données relatives au trafic afin d'identifier d'autres fournisseurs de services ainsi que le trajet emprunté par les communications liées à des infractions par logiciels rançonneurs.
Article 18 – Injonction de produire	Les injonctions de produire visées par l'article 18 peuvent être utilisées pour ordonner à une personne de produire des données informatiques stockées ayant un lien avec des infractions par logiciels rançonneurs. Cette injonction de produire peut viser des fournisseurs de services, des institutions financières, notamment des plates-formes et des prestataires de services d'actifs virtuels, et d'autres personnes morales ou physiques. Ces injonctions sont essentielles pour obtenir, par exemple, de la part de fournisseurs des données relatives aux abonnés liées aux comptes et à l'infrastructure associés aux logiciels rançonneurs.
Article 19 – Perquisition et saisie de données informatiques stockées	Les dispositions de l'article 19 relatives à la perquisition et à la saisie peuvent être utilisées pour dépister et saisir des données informatiques stockées ayant un lien avec des infractions par logiciels rançonneurs.
Article 20 – Collecte en temps réel des données relatives au trafic	Les pouvoirs conférés par l'article 20 peuvent être utilisés pour la collecte en temps réel de données relatives au trafic ayant un lien avec des infractions par logiciels rançonneurs.
Article 21 – Interception de données relatives au contenu	Les pouvoirs conférés par l'article 21 peuvent être utilisés pour l'interception de certaines données relatives au contenu ayant un lien avec des infractions par logiciels rançonneurs, par exemple des communications entre les suspects.

Ainsi, dans le cadre d'enquêtes ou de poursuites liées à des infractions par logiciels rançonneurs, les Parties peuvent recourir à la conservation rapide de données informatiques stockées, à des injonctions de produire, à la perquisition et à la saisie de données informatiques stockées, ainsi qu'à d'autres outils, afin de recueillir des preuves électroniques.

Dispositions portant sur la coopération internationale

Articles pertinents	Exemples
Principes généraux et procédures relatifs à la coopération internationale (articles 23 à 28)	Les principes généraux et les procédures de coopération internationale figurant aux articles 23 à 28 de la Convention – qui concernent l'extradition, l'entraide, etc. – sont également applicables aux infractions par logiciels rançonneurs. L'article 26 peut s'avérer particulièrement utile dans la mesure où une Partie qui possède des informations de grande valeur sur des infractions par logiciels rançonneurs obtenues dans le cadre de ses propres enquêtes peut, dans les limites de son droit interne, transmettre ces informations à l'autre Partie sans demande préalable (voir paragraphe 260 du Rapport explicatif de la Convention sur la cybercriminalité). En vertu de l'article 23 et de l'article 25, paragraphe 1, les Parties à la Convention sont tenues de coopérer entre elles, conformément aux dispositions des articles 23 à 28, « dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques » et pour « recueillir les preuves, sous forme électronique, d'une infraction pénale. »

Dispositions particulières relatives à la coopération internationale (articles 29 à 35)	Les dispositions particulières du chapitre III de la Convention peuvent être utilisées pour la coopération internationale et la collecte de preuves liées aux infractions par logiciels rançonneurs : Article 29 – Conservation rapide de données informatiques stockées Article 30 – Divulgence rapide de données conservées relatives au trafic Article 31 – Entraide concernant l'accès aux données stockées Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic Article 34 – Entraide en matière d'interception de données relatives au contenu Article 35 – Réseau 24/7
---	---

Étant donné que les infractions par logiciels rançonneurs font généralement intervenir des auteurs, des cibles et des victimes, des prestataires de services, des institutions financières ou des systèmes informatiques situés dans plusieurs juridictions, il est particulièrement important d'être efficace dans la mise en œuvre de ces dispositions de coopération internationale.

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE 224)

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE 224) a été ouvert à la signature le 12 mai 2022. Une fois en vigueur, cet instrument apportera aux Parties à ce Protocole de nouveaux outils pour le « renforcement de la coopération et de la divulgation de preuves électroniques ». Ces outils seront importants, et, dans certains cas, très importants, pour les enquêtes et procédures pénales liées à des infractions par logiciels rançonneurs. Ils comprennent :

- Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine directement auprès d'un organisme d'une autre Partie fournissant des services d'enregistrement de noms de domaine ;

- Article 7 - Divulgarion de données relatives aux abonnés par le biais d'une coopération directe avec un prestataire de services d'une autre Partie ;
- Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic ;
- Article 9 – Divulgarion accélérée de données informatiques stockées en situation d'urgence ;
- Article 10 – Demande d'entraide urgente ;
- Article 11 – Vidéoconférence ;
- Article 12 – Équipes communes d'enquête et enquêtes communes.

Le champ d'application de ce Protocole aussi est relativement vaste, dans la mesure où ce traité s'applique non seulement aux infractions pénales relatives à des systèmes et des données informatiques, mais aussi à la collecte de preuves, sous forme électronique, de toute infraction pénale (voir article 2, paragraphe 1, alinéa a).

Les conditions et sauvegardes de l'article 13 garantissent que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le Protocole sont soumis aux conditions et sauvegardes prévues par le droit interne de chaque Partie, qui doit assurer la protection adéquate des droits de l'homme et des libertés. De plus, étant donné qu'un grand nombre de Parties au Protocole peuvent être tenues, pour se conformer à leurs obligations constitutionnelles ou internationales, d'assurer la protection des données à caractère personnel, l'article 14 prévoit des garanties de protection des données pour permettre aux Parties de satisfaire à ces obligations, et garantit que des données à caractère personnel peuvent être transférées lorsqu'il est fait usage de ces formes accélérées de coopération.

Déclaration du T-CY

Le T-CY convient que :

- les infractions liées à des attaques par logiciels rançonneurs peuvent comprendre des comportements devant être érigés en infractions pénales conformément aux articles 2 à 8 et à l'article 11 (tentative et complicité), ainsi que des comportements pouvant engager la responsabilité des personnes morales en vertu de l'article 12 de la Convention sur la cybercriminalité ;

- les mesures procédurales et les outils de coopération internationale de la Convention peuvent être utilisés pour enquêter sur les attaques par logiciels rançonneurs et infractions connexes, et sur leur facilitation, la participation à ces infractions et les actions préparatoires, et pour engager des poursuites à l'encontre des auteurs ;
- une fois en vigueur, le Deuxième Protocole additionnel à la Convention sur la cybercriminalité apportera à ses Parties de nouveaux outils permettant de renforcer la coopération et la divulgation de preuves électroniques en lien avec des attaques par logiciels rançonneurs.

Note d'orientation sur la portée d'application des pouvoirs de procédure et des dispositions portant sur la coopération internationale⁷⁰

Introduction

Lors de sa 8^e session plénière (décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, y compris à la lumière des nouveautés juridiques, politiques ou techniques⁷¹. Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note concerne la portée d'application des pouvoirs de procédure au niveau national et des dispositions portant sur la coopération internationale de la Convention sur la cybercriminalité (STE n° 185) et de son Deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224).

Si le texte de la Convention sur la cybercriminalité indique clairement que les pouvoirs procéduraux et les dispositions relatives à la coopération internationale sont applicables non seulement à la cybercriminalité (articles 2 à 11 de la Convention), mais aussi « à toutes les autres infractions pénales commises au moyen d'un système informatique » et « à la collecte des preuves électroniques de toute infraction pénale » (article 14.2 b et c; et articles 23 et 25 de la STE n° 185), et bien que cela soit confirmé par le Deuxième Protocole additionnel à la Convention (article 2 de la STCE n° 224), ce champ d'application n'est pas toujours bien compris et certaines législations nationales limitent l'application des pouvoirs de procédure ou des dispositions relatives à la coopération internationale à un ensemble de cybercrimes.

Le T-CY a donc estimé que la rédaction d'une note d'orientation précisant comment les principales dispositions en matière de procédure et de coopération internationale pourraient s'appliquer non seulement aux infractions commises contre et au moyen de systèmes informatiques, mais aussi à toute une série d'infractions, présentait un intérêt pratique et stratégique.

70. Adoptée par le T-CY lors de sa 28^e réunion plénière (27-28 juin 2023).

71. Voir le mandat du T-CY (article 46 de la Convention de Budapest).

Dispositions pertinentes de la Convention sur la cybercriminalité (STE n° 185)

Dispositions procédurales

En vertu de la Convention sur la cybercriminalité, « [c]haque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes de » prendre les mesures procédurales énoncées aux articles 16 à 21 de la Convention :

- Article 16 – Conservation rapide de données informatiques stockées
- Article 17 – Conservation et divulgation rapides de données relatives au trafic
- Article 18 – Injonction de produire
- Article 19 – Perquisition et saisie de données informatiques stockées
- Article 20 – Collecte en temps réel des données relatives au trafic
- Article 21 – Interception de données relatives au contenu

Ces mesures sont soumises aux conditions et sauvegardes prévues à l'article 15.

La portée d'application de ces mesures procédurales est définie à l'article 14 :

Article 14 – Portée d'application des mesures du droit de procédure

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
2. Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
 - a. aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
 - b. à toutes les autres infractions pénales commises au moyen d'un système informatique ; et
 - c. à la collecte des preuves électroniques de toute infraction pénale.
3. a. Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

- b. Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:
 - i. qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
 - ii. qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Conformément à l'article 14.2 de la Convention, les pouvoirs de procédure sont donc applicables à la collecte de preuves sous forme électronique de toute infraction pénale. De la sorte, « les preuves électroniques de toute infraction pénale peuvent être obtenues ou collectées au moyen des pouvoirs et des procédures énoncés dans [cette] section » de la Convention (paragraphe 141 du rapport explicatif de la Convention).

Le paragraphe 3 de l'article 14 prévoit des exceptions à ce vaste champ d'application et permet aux Parties de restreindre la portée des pouvoirs plus inclusifs (comme la collecte en temps réel des données relatives au trafic (article 20) ou l'interception de données relatives au contenu (article 21)).

En conséquence, les autorités compétentes peuvent ordonner la conservation de données, ordonner la production de données, perquisitionner ou saisir des données informatiques stockées, ou ordonner ou effectuer la collecte en temps réel de données relatives au trafic ou l'interception de données relatives au contenu⁷² dans le cadre d'enquêtes pénales spécifiques liées à toute infraction prévue par le droit national, y compris par exemple⁷³:

- la corruption;
- la contrefaçon de médicaments ou d'autres infractions menaçant la santé publique, y compris les infractions liées à la COVID-19;
- les différentes formes de maltraitance des enfants;

72. Comme indiqué aux articles 20 et 21 de la Convention, la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu peuvent faire l'objet de certaines restrictions, telles que la limitation imposée aux infractions graves.

73. Voir également ci-dessous les références aux traités internationaux pertinents pour certaines de ces infractions.

- les différentes formes de violence familiale et de violence à l'égard des femmes ;
- les différentes formes d'infractions économiques et financières ;
- les infractions liées à la drogue ;
- la fraude ;
- les enlèvements ;
- la manipulation de compétitions sportives ;
- le blanchiment de capitaux et le financement du terrorisme ;
- les meurtres ;
- les infractions ayant trait au crime organisé ;
- les viols et autres formes de violence sexuelle ;
- le terrorisme ;
- les génocides, crimes contre l'humanité, crimes de guerre et autres principaux crimes internationaux ;
- la traite des êtres humains ;
- la xénophobie, le racisme et d'autres formes de discours de haine.

Dispositions relatives à la coopération internationale

Le vaste champ d'application des pouvoirs procéduraux au niveau national s'étend aux principes et aux mesures liés à la coopération internationale (chapitre III de la Convention). Les articles 23 et 25 énoncent clairement que la coopération est non seulement possible aux fins d'investigation ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques, mais aussi pour la collecte de preuves sous forme électronique de toute infraction pénale :

Article 23 – Principes généraux relatifs à la coopération internationale

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

Article 25 – Principes généraux relatifs à l'entraide

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Le paragraphe 243 du rapport explicatif de la Convention confirme par ailleurs :

« la coopération doit s'étendre à toutes les infractions pénales liées à des systèmes et données informatiques (c'est-à-dire les infractions visées par l'article 14, paragraphe 2, lettres a et b), ainsi qu'à la collecte de preuves sous forme électronique se rapportant à une infraction pénale. En d'autres termes, les clauses du chapitre III sont applicables soit aux situations où l'infraction est commise à l'aide d'un système informatique, soit à celles où une infraction ordinaire, non commise à l'aide d'un système informatique (par exemple un meurtre), donne lieu à la collecte de preuves sous forme électronique. »

Les Parties peuvent restreindre ce vaste champ d'application en ce qui concerne l'entraide dans la collecte en temps réel de données relatives au trafic (article 33) et l'entraide en matière d'interception de données relatives au contenu (article 34). En outre, la coopération internationale peut être subordonnée à certaines conditions, comme l'existence d'une double incrimination⁷⁴ ou les motifs de refus prévus aux articles 25.4 et 27.4 de la Convention.

Les principes et mesures de coopération internationale concernant les infractions énumérées dans la Convention et les autres infractions pénales commises au moyen d'un système informatique, ainsi que la collecte de preuves électroniques de toute autre infraction pénale, sont énoncés aux articles 23 à 35⁷⁵ de la Convention :

- Article 23 – Principes généraux relatifs à la coopération internationale ;
- Article 25 – Principes généraux relatifs à l'entraide ;
- Article 26 – Information spontanée ;
- Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables ;

74. Comme l'énonce le paragraphe 259 du rapport explicatif de la Convention, « [d]ans les affaires auxquelles le critère de la double incrimination est applicable, il devrait l'être d'une façon souple, de nature à faciliter l'octroi de l'assistance ».

75. Note : l'obligation d'extrader prévue à l'article 24 (Extradition) s'applique uniquement aux « infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère ».

- Article 28 – Confidentialité et restriction d'utilisation ;
- Article 29 – Conservation rapide de données informatiques stockées ;
- Article 30 – Divulgence rapide de données conservées ;
- Article 31 – Entraide concernant l'accès aux données stockées ;
- Article 32 – Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public ;
- Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic ;
- Article 34 – Entraide en matière d'interception de données relatives au contenu ;
- Article 35 – Réseau 24/7.

Les Parties à la Convention peuvent recourir à ces mesures et principes pour coopérer entre elles dans toute la mesure possible aux fins d'investigations ou de procédures et de collecte de preuves sous forme électronique de toute infraction pénale, et demander la conservation des données, l'accès à des données informatiques stockées, la collecte en temps réel de données relatives au trafic ou l'interception de données relatives au contenu⁷⁶, ou encore l'accès transfrontalier à des données informatiques stockées en ce qui concerne toute infraction pénale et dans les conditions prévues au chapitre III de la Convention.

Dispositions pertinentes du Deuxième Protocole additionnel (STCE n° 224)

Le Deuxième Protocole additionnel à la Convention sur la cybercriminalité (STCE n° 224) a été ouvert à la signature le 12 mai 2022. Après son entrée en vigueur, cet instrument offrira aux Parties des outils supplémentaires pour « renforcer la coopération et la divulgation des preuves électroniques ».

Ce protocole a lui aussi un vaste champ d'application et s'applique non seulement aux infractions pénales liées aux systèmes et aux données informatiques,

76. Comme indiqué aux articles 20 et 21 de la Convention, la collecte en temps réel de données relatives au trafic et l'interception de données relatives au contenu peuvent faire l'objet de certaines restrictions, telles que la limitation imposée aux infractions graves. En ce qui concerne les articles 33 et 34 sur la coopération internationale, « [c]haque partie accorde cette assistance au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne » (article 33.2), et s'agissant de l'interception des données relatives au contenu, « [l]es Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables [...] » (article 34).

mais également à la collecte de preuves sous forme électronique de toute infraction pénale :

Article 2 – Champ d'application

1. Sauf dispositions contraires prévues au présent Protocole, les mesures qu'il énonce s'appliquent :
 - a. pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique ; et
 - b. pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole.

Les mesures prévues par ce Protocole sont les suivantes :

- Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine directement auprès d'une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie ;
- Article 7 – Divulgarion de données relatives aux abonnés par le biais d'une coopération directe avec un fournisseur situé sur le territoire d'une autre Partie ;
- Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic ;
- Article 9 – Divulgarion accélérée de données informatiques stockées en situation d'urgence ;
- Article 10 – Demande d'entraide urgente ;
- Article 11 – Vidéoconférence ;
- Article 12 – Équipes communes d'enquête et enquêtes communes.

Ces mesures sont soumises aux conditions et sauvegardes prévues aux articles 13 et 14 de la STCE n° 224.

Les autorités compétentes peuvent donc demander des informations sur l'enregistrement des noms de domaine, ordonner la divulgation d'informations relatives aux abonnés, donner suite à des injonctions de production d'informations sur les abonnés et de données relatives au trafic, coopérer en cas d'urgence, recourir à la vidéoconférence ou mettre en place des équipes

communes d'enquête ou participer à des enquêtes communes liées à des enquêtes ou à des procédures pénales concernant des infractions pénales en rapport avec des systèmes et des données informatiques ainsi que la collecte de preuves sous forme électronique de toute infraction.

Synergies entre la Convention sur la cybercriminalité et d'autres traités

Les pouvoirs procéduraux au niveau national et les principes et mesures de coopération internationale peuvent également être utilisés pour recueillir des preuves électroniques relatives à des infractions prévues par d'autres accords internationaux auxquels les États sont Parties, sous réserve des conditions pertinentes mentionnées plus haut⁷⁷. Ces accords peuvent porter sur la corruption⁷⁸; la contrefaçon de médicaments ou d'autres infractions menaçant la santé publique⁷⁹; la maltraitance des enfants⁸⁰; la violence domestique et la violence à l'égard des femmes⁸¹; les infractions liées à la drogue⁸²; la manipulation de compétitions sportives⁸³; le blanchiment de capitaux et le financement du terrorisme⁸⁴; les infractions liées à la criminalité organisée⁸⁵; le terrorisme⁸⁶;

77. Telles que l'existence d'une double incrimination ou les motifs de refus prévus aux articles 25.4 et 27.4 de la Convention.

78. Par exemple, les actes criminels couverts par la [Convention pénale sur la corruption](#) (STE n° 173) du Conseil de l'Europe ou la [Convention des Nations Unies contre la corruption](#).

79. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe sur la contrefaçon des produits médicaux et les infractions similaires menaçant la santé publique](#) (STCE n° 211).

80. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels](#) (STCE n° 201).

81. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique](#) (STCE n° 210).

82. Par exemple, les actes criminels couverts par les [Conventions Internationales sur le Contrôle des Drogues](#).

83. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe sur la manipulation de compétitions sportives](#) (STCE n° 215).

84. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et au financement du terrorisme](#) (STCE n° 198).

85. Par exemple, les actes criminels couverts par la [Convention des Nations Unies contre la criminalité transnationale organisée](#) et les protocoles s'y rapportant.

86. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe pour la prévention du terrorisme](#) (STCE n° 196) et les protocoles s'y rapportant.

la traite des êtres humains⁸⁷; ou le génocide, les crimes contre l'humanité, les crimes de guerre et autres principaux crimes internationaux⁸⁸.

Pour les Parties au premier Protocole additionnel à la Convention sur la cybercriminalité relatif aux actes de xénophobie et de racisme commis par le biais de systèmes informatiques (STE n° 189)⁸⁹, l'article 8.2 indique que les « Parties étendent le champ d'application des mesures définies aux articles 14 à 21 et 23 à 35 de la Convention, aux articles 2 à 7 de ce Protocole ».

En 2018, le T-CY a recommandé que les Parties à la Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels (STCE n° 201) et à la Convention d'Istanbul sur la violence contre les femmes et la violence domestique (STCE n° 210) soient encouragées à « introduire dans leur droit interne les pouvoirs procéduraux prévus aux articles 16 à 21 de la Convention de Budapest et de devenir parties à la Convention de Budapest pour faciliter la coopération internationale en matière de preuve électronique (articles 23 à 35 de la Convention de Budapest) en relation avec la violence sexuelle en ligne contre les enfants »⁹⁰.

Déclaration du T-CY

Le T-CY convient que les dispositions de droit procédural et les principes et mesures de la coopération internationale de la Convention sur la cybercriminalité sont applicables non seulement aux infractions liées aux systèmes et données informatiques, mais aussi à la collecte de preuves électroniques de toute infraction pénale. Ce vaste champ d'application s'applique également aux mesures prévues par le Deuxième Protocole additionnel à la Convention.

Ce champ d'application permet en outre de dégager des synergies entre la Convention de Budapest et d'autres accords internationaux.

Note d'orientation T-CY n° 14

87. Par exemple, les actes criminels couverts par la [Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains](#) (STCE n° 197).

88. Par exemple, les actes criminels couverts par la [Convention pour la prévention et la répression du crime de génocide](#) de 1948, les [quatre Conventions de Genève sur le droit international humanitaire](#) et leurs protocoles additionnels de 1949, ou le [Statut de Rome de la Cour pénale internationale](#).

89. [Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques](#) (STE n° 189).

90. Voir l'étude cartographique du T-CY sur la cyberviolence <https://rm.coe.int/t-cy-2017-10-cbg-study-fr-v2/1680993e65>

Information spontanée⁹¹ (Article 26 de la Convention sur la cybercriminalité)

Introduction

Lors de sa 8^{ème} session plénière (décembre 2012), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de publier des [notes d'orientation](#) destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, y compris à la lumière des nouveautés juridiques, politiques ou techniques.⁹² Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties. Les notes d'orientation représentent l'interprétation commune des Parties à ce traité concernant l'utilisation de la Convention.

Les autorités de justice pénale d'une juridiction peuvent détenir des informations qu'elles estiment susceptibles d'aider une autre Partie dans le cadre d'une enquête ou d'une procédure pénale, mais dans certains cas, la Partie chargée de l'enquête peut ne pas être au courant de l'existence de ces informations. L'article 26 de la Convention fournit une base juridique pour la transmission de ces informations à l'autre Partie en l'absence de demande préalable.

L'importance de l'article 26 s'est accrue au fil du temps, notamment dans le cadre d'enquêtes impliquant le dark web ou la collecte de grandes quantités de données obtenues à partir de communications. Dans le même temps, toutes les Parties n'exploitent pas de manière cohérente toutes les possibilités offertes par cette disposition.

Le T-CY a donc décidé que des orientations sur l'article 26 s'inspirant des pratiques actuelles des Parties dans l'application de l'article 26 seraient utiles et permettraient aux Parties de tirer pleinement parti du potentiel de la Convention en ce qui concerne les informations spontanées.

La présente note aborde donc les aspects essentiels (a) du transfert d'informations spontanées et (b) de leur utilisation dans la Partie destinataire lorsqu'elles sont obtenues sur la base de l'article 26, y compris la question de savoir si les informations reçues peuvent ou non être utilisées comme éléments de preuve lorsqu'elles sont reçues sur la base de cet article.

La présente note se fonde également sur les résultats des réponses au

91. Adoptée par le T-CY suite à la 32^e plénière par procédure d'approbation tacite (25 juin 2025)

92. Voir le mandat du T-CY (article 46 de la Convention sur la cybercriminalité).

questionnaire⁹³ reçues des Parties avant janvier 2025, sur les résultats d'un événement conjoint sur les «informations spontanées» organisé en coopération avec Eurojust à La Haye, sur un rapport de base⁹⁴ et sur les discussions tenues lors de la conférence Octopus à Bucarest en 2023⁹⁵.

Article 26 Convention sur la cybercriminalité

Texte de la disposition :

Article 26 - Information spontanée

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

Extrait du rapport explicatif :

260. Cet article a été établi sur la base de dispositions d'instruments antérieurs du Conseil de l'Europe telles que l'article 10 de la Convention relative au blanchiment, au dépistage, à la saisie et la confiscation des produits du crime (STE n° 141) et l'article 28 de la Convention pénale sur la corruption (STE n° 173). Il arrive de plus en plus souvent qu'une partie possède des informations précieuses dont elle estime qu'elles pourraient présenter un intérêt pour l'enquête ou la procédure ouverte ou engagée dans une autre Partie et dont celle-ci n'a pas connaissance. En pareil cas, aucune demande d'entraide n'est présentée.

93. Un questionnaire sur les pratiques des Parties à la Convention a été envoyé aux représentants de T-CY en juillet 2024.

94. Secrétariat du T-CY et Bureau du programme sur la cybercriminalité du Conseil de l'Europe «Spontaneous information» - Current practices of the use of Article 26, présenté lors de la 31^{ème} plénière du T-CY (11-12 décembre 2024) et mis à jour en mai 2025 (document T-CY (2024)11 rev) (disponible en anglais uniquement).

95. La conférence Octopus 2023 (13 décembre 2023) a proposé un atelier sur le partage spontané d'informations.

Le paragraphe 1 habilite l'État qui possède l'information en question à la communiquer à l'autre État sans que celui-ci lui en ait fait la demande au préalable. On a jugé bon d'insérer cette disposition car, en application de la législation de certains États, une telle habilitation positive est nécessaire pour pouvoir accorder l'entraide en l'absence d'une demande. Une Partie n'est pas tenue de communiquer spontanément des informations à une autre Partie ; elle a toute latitude pour le faire en fonction des circonstances de l'espèce. De plus, la divulgation spontanée d'informations n'interdit pas à la Partie qui les communique, si elle a compétence pour le faire, d'ouvrir une enquête ou d'engager une procédure au sujet des faits ainsi divulgués.

261. Le paragraphe 2 traite du fait que dans certains cas, une Partie ne communiquera spontanément des informations que si les informations sensibles restent confidentielles ou si elles sont utilisées sous certaines autres conditions. En particulier, la confidentialité sera un facteur important dans les affaires où d'importants intérêts de l'État communiquant les informations pourraient être mis en péril si celles-ci étaient rendues publiques, par exemple s'il y a lieu de ne pas révéler une méthode de collecte de l'information ou le fait qu'une association de malfaiteurs fait l'objet d'une enquête. Si, renseignements pris au préalable, il s'avère que la Partie destinataire ne peut pas respecter la condition mise par l'autre Partie à l'utilisation des informations (si, par exemple, elle ne peut pas respecter à la demande de confidentialité parce que les informations en questions doivent être utilisées à titre de preuves lors d'un procès public), elle doit en informer l'autre Partie, qui peut alors décider de communiquer ces informations ou de ne pas le faire. Si, toutefois, la Partie destinataire accepte la condition fixée, elle doit s'y plier. On prévoit que les conditions imposées par cet article seraient compatibles avec celle que pourrait fixer la Partie communiquant les informations à la suite d'une demande d'entraide présentée par la Partie destinataire.

3. Interprétation par le T-CY de l'article 26 de la Convention sur la cybercriminalité

3.1. Champ d'application de l'article 26, considérations générales et sauvegardes

3.1.1. Caractère discrétionnaire de l'article 26

L'article 26 fournit une base juridique permettant à une Partie de transmettre à une autre Partie des informations obtenues au cours de sa propre enquête.

La disposition laisse à la discrétion d'une Partie («une Partie peut (...)») le soin de transmettre ou non les informations à une autre Partie. Une Partie n'est pas obligée de transmettre spontanément des informations à une autre Partie ;

elle peut exercer son pouvoir d'appréciation à la lumière des circonstances de l'espèce.

3.1.2. Sur les notions de «spontanée» et «en l'absence de demande préalable»

La notion de «spontanée» implique que la Partie transmet les informations obtenues au cours de ses propres enquêtes internes volontairement ou de sa propre initiative, en l'absence de demande préalable de la part d'une autre Partie.

Cela n'exclut pas la possibilité de consultations informelles entre les Parties avant l'échange d'informations spontanées. Ces consultations peuvent, par exemple, porter sur des conditions spécifiques que la Partie qui fournit les données peut souhaiter imposer, ou sur des questions telles que la communication des raisons pour lesquelles, dans un cas particulier, il serait préférable de transmettre les données en vertu de l'article 26 plutôt que par le biais des procédures d'entraide.

Dans le même temps, les Parties peuvent également juger utile d'organiser une consultation de suivi après qu'une Partie a reçu des informations transmises dans le cadre d'un échange spontané. Les résultats du questionnaire ont montré que les Parties procédaient souvent à des consultations ultérieures, après la communication initiale, pour discuter des détails et de la nécessité d'une nouvelle communication d'informations spontanées. Si les Parties en conviennent, elles peuvent continuer à échanger des informations relatives à l'affaire qui a déclenché la transmission initiale, également en vertu de l'article 26. Si elles le jugent plus approprié, les Parties peuvent décider d'échanger des informations futures par le biais de procédures d'assistance mutuelle.

3.1.3. Sur le concept d'«information»

La Partie émettrice peut transmettre toute information pertinente obtenue au cours de sa propre enquête. Dans ce contexte, le terme «information» est entendu au sens large et peut prendre la forme de données informatiques ou toute autre forme.

Les Parties peuvent transmettre différents types d'informations dans le cadre de la procédure prévue à l'article 26. Dans leurs réponses au questionnaire, les Parties ont donné les exemples suivants :

- les informations recueillies au cours d'une enquête nationale ;
- les informations des services de renseignement de la police ;

- rapports sur la criminalité;
- l'identité des auteurs ou des victimes ou d'autres informations sur la commission d'un acte;
- les rapports d'audition de témoins;
- les rapports d'incidents,
- les vulnérabilités et les exploits en matière de cybersécurité;
- les adresses de protocole Internet (IP), les courriels, les comptes de médias sociaux ou les services de messagerie instantanée associés à une cyberattaque;
- des informations relatives aux comptes bancaires telles que l'IBAN ou les relevés bancaires des victimes (ou des Parties de ces relevés);
- l'enregistrement et d'autres documents sans contenu associés aux comptes utilisés dans le cadre des crimes faisant l'objet de l'enquête;
- le contenu des communications.

Les informations transmises peuvent être sous forme de données informatiques ou sous toute autre forme déterminée par la Partie qui transmet les informations.

3.1.4. Sur les notions d'«engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention» et de «pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre»

Une Partie peut envisager de transmettre spontanément à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes dans les conditions suivantes:

- ces informations pourraient aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention; ou
- ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

L'article 23⁹⁶, qui énonce les principes généraux de la coopération internationale, précise que la coopération n'est pas seulement possible aux fins d'investigations ou de procédures concernant les infractions pénales liées

96. Les articles 23 et 26 relèvent tous deux du même chapitre 3 de la Convention, ce qui rend l'article 23 pleinement applicable à l'article 26.

à des systèmes et des données informatiques, mais aussi pour recueillir les preuves, sous forme électronique, de toute infraction pénale :

Article 23 - Principes généraux relatifs à la coopération internationale

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

Ce champ d'application large s'applique également à l'article 26. En pratique, les Parties fournissent spontanément des informations au titre de l'article 26 pour toute infraction pénale ; elles ne se limitent pas aux infractions liées aux systèmes informatiques ou aux données.

En outre, les Parties fournissent spontanément des informations à diverses fins. Il s'agit notamment d'informations susceptibles d'aider l'État destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales, d'informations susceptibles d'empêcher la commission d'une infraction ou d'informations susceptibles de conduire à une demande d'entraide de la part de l'État destinataire. En général, les Parties fournissent toute information lorsqu'elles la jugent pertinente. Il appartient à la Partie destinataire de décider de l'utilisation des informations reçues, sous réserve des conditions imposées par la Partie qui a fourni les informations.

3.1.5. Sur la notion de «dans les limites de son droit interne»

Pour décider de transmettre ou non des informations à une autre Partie, une Partie doit être guidée par «les limites de son droit interne». En fonction de leur législation nationale, les Parties ont la possibilité de prévoir de telles limites. Ces limites comprennent des conditions et des garanties conformément à l'article 15 de la Convention⁹⁷.

Il est également supposé que la Partie qui fournit l'information et la Partie qui reçoit l'information respectent l'État de droit et les principes des droits humains, conformément à l'article 15 de la Convention.

Article 15 - Conditions et sauvegardes

97. Y compris les informations confidentielles/restreintes en raison de privilèges juridiques, d'immunités et de la protection des témoins, etc. sur la base du paragraphe 147 du rapport explicatif de la Convention.

- 1 - Chaque 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, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.
- 2 - Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.
- 3 - Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

3.2. Autorités jugées compétentes conformément à l'article 26

Certaines dispositions du chapitre III de la convention (par exemple, l'article 24 sur l'extradition ou l'article 27 sur les procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables) exigent des Parties qu'elles désignent des autorités pour ces types spécifiques de coopération.

L'article 26 ne contient pas une telle exigence et fait référence à une «Partie». La disposition laisse à la discrétion d'une Partie le choix des autorités qu'elle considère comme compétentes pour transmettre des informations à une autre Partie.

La pratique des Parties à la Convention indique un large éventail d'autorités transmettant les informations. Il s'agit notamment des autorités policières, des procureurs et des juges. Dans certains cas, l'échange d'informations spontanées peut commencer par une coopération de police à police⁹⁸ et se transformer en coopération judiciaire lorsque les informations échangées font partie d'une procédure judiciaire formelle et sont utilisées comme preuves devant un tribunal.

98. Toutefois, d'autres conditions spécifiques peuvent être exigées par certaines Parties pour que les informations obtenues grâce à la coopération policière puissent être utilisées comme éléments de preuve dans une procédure pénale dans la Partie destinataire.

D'après les résultats du questionnaire, certaines Parties ont également recours à la communication directe entre les autorités compétentes. Ce qui peut commencer par un premier contact entre les autorités centrales peut évoluer vers des échanges directs. Toutefois, certaines Parties préfèrent la communication/coordination par l'intermédiaire des autorités centrales, qui peuvent fournir à leurs autorités nationales les orientations nécessaires sur les lois et conditions applicables.

Les résultats du questionnaire ont également révélé que les Parties utilisent divers canaux nationaux (par exemple, le réseau 24/7 des points de contact⁹⁹ ou les autorités centrales) pour transmettre des informations en vertu de l'article 26 ou des canaux internationaux (par exemple, INTERPOL, EUROJUST, EUROPOL) pour transmettre de telles informations.

3.3. Confidentialité et autres conditions

3.3.1. Confidentialité

Conformément à l'article 26.2 de la Convention, une Partie peut subordonner la fourniture spontanée d'informations à la condition que les informations sensibles restent confidentielles ou que d'autres conditions soient imposées à l'utilisation des informations, y compris par exemple des délais, c'est-à-dire de ne pas utiliser les informations en tant que telles avant que le dossier pénal ne soit porté devant les tribunaux de la Partie qui les fournit.

La confidentialité est l'une des conditions les plus fréquemment imposées par les Parties pour garantir la confidentialité de l'enquête ou de la procédure de la Partie qui fournit l'information.

La confidentialité sera « un facteur important dans les affaires où d'importants intérêts de l'État communiquant les informations pourraient être mis en péril si celles-ci étaient rendues publiques, par exemple s'il y a lieu de ne pas révéler une méthode de collecte de l'information ou le fait qu'une association de malfaiteurs fait l'objet d'une enquête. » (paragraphe 261 du Rapport explicatif de la Convention).

3.3.2. Autres conditions

Les Parties peuvent subordonner la divulgation spontanée d'informations à des conditions supplémentaires, qui peuvent être déterminées au cas par cas.

99. Voir l'article 35 de la Convention de Budapest sur la cybercriminalité.

Si les Parties peuvent imposer une grande variété de conditions en vertu de cet article, il est prévu que les conditions imposées en vertu de cet article seraient compatibles avec celle que pourrait fixer la Partie communiquant les informations à la suite d'une demande d'entraide présentée par la Partie destinataire (paragraphe 261 du Rapport explicatif de la Convention).

Les réponses des Parties au questionnaire et le retour d'information des Parties au cours du processus de rédaction de la présente note d'orientation ont révélé que les conditions peuvent inclure, par exemple, des conditions qui ne sont pas contraires aux accords ou arrangements conclus entre les Parties concernées :

- ne pas utiliser les informations fournies à d'autres fins que celles pour lesquelles elles ont été fournies (si la finalité est précisée) ;
- ne pas transférer les informations vers un autre pays sans accord préalable ;
- n'utiliser ces informations que pour engager une procédure ou présenter une future demande d'entraide ;
- respecter les conditions de protection des données ;
- réciprocité : garantie qu'en cas de cas similaire futur, si la Partie a obtenu des informations pertinentes dans le cadre de ses propres enquêtes, elle fera tous les efforts raisonnables pour appliquer la procédure prévue à l'article 26 et transmettre les informations pertinentes à la Partie qui a imposé la condition de réciprocité préalable ;
- ne pas utiliser les informations comme éléments de preuve dans le cadre d'une procédure pénale ;
- garantir une utilisation appropriée et légale des informations ;
- fournir une notification concernant l'utilisation ultérieure/le suivi de la manière dont les informations ont été utilisées ;
- utiliser les informations uniquement pour enquêter sur la commission d'un délit et dans le cadre d'une procédure pénale ;
- notifier à la Partie qui fournit l'information, ou obtenir son autorisation, avant toute utilisation susceptible de rendre l'information publique ;
- ne pas utiliser les informations à des fins de procédures qui violent les droits et garanties fondamentaux ;
- utiliser les informations dans les conditions prévues par les traités multilatéraux ou bilatéraux ;
- utiliser les informations conformément à d'autres conditions spécifiées par les autorités/ selon le cas ;

- une clause d'anonymat : sauf dans des circonstances très exceptionnelles, à déterminer conformément au droit interne de la Partie qui fournit l'information, cette Partie ne fournira pas d'informations sur l'identité des agents enquêteurs et/ou n'accédera pas aux demandes de déclaration des agents enquêteurs, que ce soit lors d'une audience devant un tribunal ou ailleurs.

Il convient toutefois de noter qu'en vertu de l'article 26, l'imposition de conditions n'est pas obligatoire et la Partie qui fournit les informations peut décider de ne pas imposer de conditions à l'utilisation des informations dans la Partie destinataire si elle ne les juge pas nécessaires dans un cas particulier. La décision de divulguer ou non l'information, et dans quelles conditions, est laissée à l'appréciation de la Partie qui fournit l'information.

3.3.3. Utilisation des informations comme éléments de preuve dans le cadre de procédures pénales dans la Partie destinataire

La Partie qui fournit les informations peut subordonner leur divulgation à la condition qu'elles ne soient pas utilisées comme éléments de preuve dans le cadre d'une procédure pénale dans la Partie destinataire. La Partie qui divulgue les informations peut également imposer d'autres conditions appropriées qui, si elles sont remplies, permettront l'utilisation des informations comme éléments de preuve dans la Partie destinataire, dans la mesure où cela est compatible avec son droit interne. Un exemple d'une telle condition serait l'obligation imposée à la Partie destinataire de rechercher et d'obtenir les informations partagées en vertu de l'article 26 également par le biais d'une procédure d'entraide avant qu'elles puissent être utilisées comme éléments de preuve dans le cadre d'une procédure pénale dans la Partie destinataire.

Toutefois, si aucune condition de ce type n'est imposée, la Partie destinataire peut utiliser les informations comme éléments de preuve dans le cadre d'une procédure pénale, dans la mesure où cela est compatible avec son droit interne. Cette approche est conforme à la Convention.

Dans certaines Parties, le droit interne permet d'utiliser les informations spontanées reçues comme éléments de preuve dans une procédure pénale si cela est conforme au droit interne de la Partie qui les fournit ou si cette Partie a donné son autorisation ou son consentement. En cas d'ambiguïté, les Parties ont généralement recours à la consultation.

L'article 26 ne contient aucune règle sur l'admissibilité des preuves et le T-CY considère qu'il s'agit d'une question relevant du droit interne. La consultation

entre les Parties peut réduire le risque que les informations transférées soient irrecevables dans la Partie destinataire.

Il convient également de noter que la Partie émettrice ne peut pas obliger la Partie destinataire à utiliser l'information comme élément de preuve dans la procédure pénale de cette dernière. Le droit interne de la Partie destinataire peut prévoir diverses conditions et restrictions concernant le type d'informations pouvant être utilisées comme preuves électroniques dans ses procédures pénales. Le droit interne de certaines Parties peut exclure l'utilisation d'informations reçues spontanément comme éléments de preuve dans une procédure pénale, par exemple dans les cas suivants :

- les informations ont été obtenues par un canal ou auprès d'une autorité que le droit interne ne considère pas comme compétente pour l'échange de preuves (par exemple, les informations obtenues dans le cadre d'une coopération entre services de police) ;
- les informations ont été obtenues d'une manière incompatible avec le droit interne régissant cette obtention dans la Partie destinataire ;
- les informations ne peuvent être utilisées que dans un but précis, tel que la prévention d'une menace imminente et grave pour la sécurité publique ;
- sont en grande partie des rumeurs et aucune source originale ne peut être identifiée pour en confirmer la véracité ou l'authenticité ;
- les informations sont plus sensibles (par exemple, des procédures différentes sont requises pour des types de données plus sensibles telles que les données sur le contenu ou les données liées au secret bancaire).

Par conséquent, il peut être utile pour les deux Parties de se consulter sur la manière dont les informations seront spontanément partagées afin de maximiser les possibilités d'utilisation sans qu'il soit nécessaire de recourir à des demandes ou à des procédures supplémentaires. Toutefois, si la Partie destinataire est tenue, en vertu de son droit interne, d'obtenir les informations par d'autres moyens afin de pouvoir les utiliser comme éléments de preuve dans une procédure pénale, par exemple en les obtenant par le biais d'une procédure d'entraide auprès de l'autorité centrale officiellement désignée, la Partie qui a spontanément fourni les informations devrait respecter ces exigences. Cette Partie ne devrait pas refuser d'exécuter une demande d'entraide ultérieure au seul motif qu'elle a déjà fourni les informations par divulgation spontanée. En outre, en particulier dans les cas où une demande d'entraide ultérieure est prévue, il peut être utile d'indiquer clairement quelles

informations ont été précédemment partagées en vertu de l'article 26 (par exemple, en utilisant des fichiers zippés et des valeurs de hachage), afin que ces données puissent être facilement reproduites par la Partie qui a fourni les informations en réponse à la demande formelle d'entraide.

3.4. Consultation et suivi

Si la Partie destinataire ne peut se conformer à une condition demandée par la Partie qui fournit l'information (par exemple, si elle ne peut se conformer à une condition de confidentialité parce que l'information est nécessaire comme preuve dans un procès public dans la Partie destinataire), la Partie destinataire en informe la Partie qui fournit l'information, qui a alors la possibilité de ne pas fournir l'information. Si, toutefois, la Partie destinataire accepte la condition fixée, elle doit s'y plier (paragraphe 261 du rapport explicatif de la convention).

L'article 26 prévoit donc la possibilité d'une consultation entre les Parties lorsqu'il s'agit d'informer la Partie qui fournit l'information qu'une condition ne peut être respectée.

Toutefois, cette consultation peut également être utile dans les cas où aucune condition spécifique n'a été imposée. Par exemple, elle peut servir à déterminer si les informations spécifiques fournies spontanément peuvent être utilisées comme éléments de preuve dans une procédure pénale dans la Partie destinataire, si cela n'était pas clair au moment où les informations ont été fournies.

En outre, dans le cadre des bonnes pratiques, de nombreuses Parties utilisent ces consultations pour assurer le suivi avec les Parties auprès desquelles les informations ont été obtenues, afin de les tenir informées de la manière dont les informations ont été traitées.

Ceci est utile pour maintenir une coopération étroite avec une autre Partie. Ce suivi peut être assuré à la demande expresse de la Partie qui fournit des informations spontanées, mais il n'est pas limité à ces seuls cas.

La pratique a montré qu'un suivi avec la Partie qui a fourni l'information peut être utile dans les situations suivantes :

- au cours d'une enquête ouverte ou menée sur la base d'informations fournies spontanément, de nouvelles informations sont obtenues qui peuvent être pertinentes pour la Partie qui les a fournies ou pour une autre Partie ;
- l'ouverture ou le refus d'une enquête pénale (poursuites) sur la base des informations obtenues ;

- si les informations ont donné lieu à une enquête plus approfondie ou si elles sont utiles à celle-ci, et quel est l'état d'avancement de l'enquête;
- lorsqu'une coopération supplémentaire est nécessaire parce que certains éléments d'information sont manquants;
- lorsque la décision finale (arrêt définitif) est rendue par la juridiction.

Sauf si la Partie qui fournit l'information le demande expressément, il appartient à la Partie qui reçoit l'information spontanée de déterminer si et dans quels cas un suivi sera assuré.

La pratique a également montré que les Parties utilisent également des canaux informels à des fins de suivi, y compris l'utilisation de communications orales ou électroniques.

3.5. Exemples d'utilisation d'informations spontanées

- Les autorités de la Partie 1 qui enquêtent sur un forum en ligne pour l'échange de matériel relatif à l'exploitation et aux abus sexuels concernant des enfants découvrent qu'un membre de ce forum communique à partir d'une adresse IP située dans la Partie 2. Les autorités de la Partie 1 peuvent utiliser l'article 26 pour partager cette information avec les autorités de la Partie 2, qui peuvent alors ouvrir leur propre enquête sur ce membre. Bien que ces informations soient partagées par les autorités de la Partie 1 sans demande d'entraide, la Partie 2 destinataire peut décider de faire suivre cette information d'une demande d'entraide si son droit interne l'exige afin d'utiliser ces informations comme éléments de preuve dans des procédures pénales ultérieures.
- Dans le cadre de leurs enquêtes, les autorités d'une Partie ont récupéré un très grand nombre de données relatives à des communications entre des auteurs d'infractions relevant de plusieurs juridictions, y compris des auteurs d'infractions dans d'autres Parties. Elles peuvent utiliser l'article 26 pour partager ces informations avec les autorités de ces autres Parties - sans demande d'entraide - qui peuvent alors entamer leurs propres enquêtes.
- Les autorités d'une Partie reçoivent une notification d'une personne morale sur leur territoire concernant l'accès illégal et l'interférence de données, après avoir identifié une perte significative de données qui pourrait indiquer la préparation d'un ransomware. Après enquête, elles découvrent que le suspect est d'une autre juridiction d'où proviennent les attaques. L'échange d'informations au titre de l'article 26 est une mesure

importante qui permet aux autorités de la deuxième Partie d'entamer leur propre enquête et de mettre fin à l'activité criminelle.

- Les autorités d'une Partie enquêtent sur un cas de fraude informatique impliquant des auteurs et des victimes, y compris dans plusieurs juridictions d'autres Parties, dont les données financières ont été compromises. Le partage d'informations spontanées avec les autorités de ces autres Parties peut leur permettre d'ouvrir leurs propres enquêtes et d'identifier les victimes sur leur territoire. Parallèlement, une Partie peut, lorsqu'elle fournit des informations spontanées, demander à la Partie destinataire d'assurer un suivi si cette dernière dispose d'informations susceptibles d'être utiles dans le cadre d'enquêtes ou de procédures pénales dans la Partie qui fournit les informations spontanées.
- L'article 26 peut constituer un outil particulièrement utile et efficace pour l'échange d'informations spontanées indiquant un risque important et imminent pour la vie ou la sécurité de toute personne physique¹⁰⁰ dans une autre Partie. Ces situations d'urgence peuvent inclure des actes de terrorisme, des enlèvements ou l'exploitation et l'abus sexuels d'enfants. L'échange d'informations spontanées peut aider à identifier et à sauver les victimes de crimes graves. La Partie qui partage l'information peut, par exemple, imposer la condition que l'information ne puisse être utilisée que pour faire face à une situation d'urgence.

4. Déclaration T-CY

Le T-CY convient que ce qui précède représente l'interprétation commune des Parties quant à la portée et aux éléments de l'article 26 de la Convention sur les informations spontanées.

L'article 26 constitue une base juridique positive permettant à une Partie de partager des informations qu'elle a obtenues dans le cadre de sa propre enquête avec une autre Partie sans demande préalable d'entraide, lorsqu'elle considère que la divulgation de ces informations pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures, ou qu'elle pourrait conduire à une demande de coopération de la part de cette Partie. La Partie destinataire peut utiliser les informations comme éléments de preuve dans le cadre d'une procédure pénale, à moins que cette possibilité

100. Défini comme «urgence» à l'article 3.2.c du Deuxième Protocole Additionnel à la Convention sur la cybercriminalité (STCE 224).

ne soit exclue par des conditions imposées par la Partie émettrice ou qu'elle ne soit contraire au droit interne de la Partie destinataire.

Compte tenu des avantages que l'article 26 peut offrir, les Parties sont encouragées à examiner comment la procédure d'«information spontanée» prévue par cet article peut être utilisée efficacement par leurs autorités.

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits humains du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits humains, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE