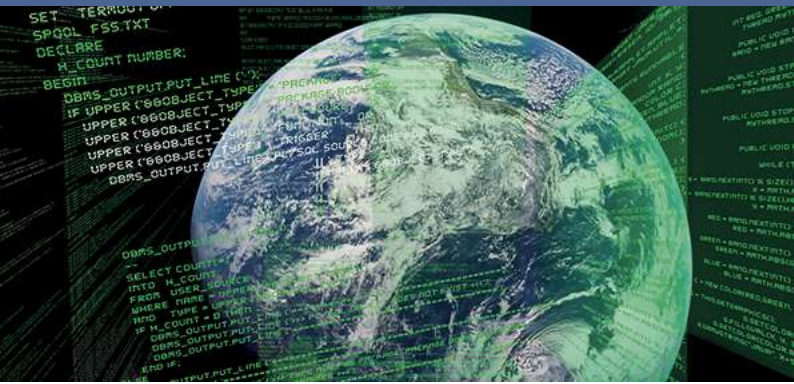
CONVENTION SUR LA CYBERCRIMINALITÉ

PROTOCOLE SUR LA XÉNOPHOBIE ET LE RACISME



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

rapports explicatifs
et notes d'orientation

Convention sur la cybercriminalité (STE nº 185)

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 cyberespace, 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 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 cyberespace, 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 21e 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 23e 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 2e 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 enfantine

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 enfantine en vue de sa diffusion par le biais d'un système informatique ;

b. l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;

c. la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;

d. le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

e. la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2. Aux fins du paragraphe 1 ci-dessus, le terme « pornographie enfantine » 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 présence 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 habiliter 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 – Divulgation 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'accep-

tation 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 constituants 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 constituants 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 constituants, 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

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 109e 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) 9[2] concernant le droit matériel et dans la Recommandation n° R (95) 13[3] relative aux problèmes de procédure pénale liés aux technologies de l'information.

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

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

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.

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 fonction-

nement 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 583e 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 21e 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 23e 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 2e 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 50e 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 contremesure. 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 nº (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 le 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 nº (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 2e 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 enfantine 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 enfantine 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 enfantine, 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 enfantine 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 enfantine. 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 enfantine). 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 nº 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.

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^{os} 1, 4, 6, 7 et 12 (STE n^{o} 005[4], 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

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 1er 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 1er novembre 1998. A compter de cette date, le Protocole n° 9 (STE n° 140), entré en vigueur le 1er octobre 1994, est abrogé et le Protocole n° 10 (STE n° 146) est devenu sans objet.

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 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 raisonnabilité 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 instaurées 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 enfantine, 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 habiliter 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'usager 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 q'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 enfantine. 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 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-divulgation 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'usagers 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 enfantine. 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, subsidiarité 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

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.

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 enfantine). 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 des conséquences désastreuses sur le bon fonctionnement des systèmes informatiques. En cas de diffusion illicite de pornographie enfantine, 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 illicites. 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 enfantine). 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'une 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^{os} 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. Etant 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.

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 toute 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 informatique stockées), avoir la capacité de le faire à des fins nationales. Le paragraphe 1 autorise une Partie à demander ce type d'entraide et le paragraphe 2 exige de la Partie requise qu'elle se donne les moyens de la fournir. Par ailleurs, le paragraphe 2 est conforme au principe selon lequel les conditions dans lesquelles cette coopération doit être fournie sont celles qu'énoncent les traités, arrangements et législations nationales applicables concernant l'entraide judiciaire en matière pénale. En vertu du paragraphe 3, il doit être satisfait rapidement à une telle demande lorsque 1) il y a des raisons de penser que les données pertinentes sont particulièrement susceptibles de perte ou de modification, ou 2) les traités, arrangements ou législations prévoient une coopération rapide.

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 Partie 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 nº 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 315e 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 être 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 internationaux[11]. 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 Constitution ou d'autres principes fondamentaux concernant la séparation des pouvoirs en matière de justice pénale entre le gouvernement central et les Etats constituants 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

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.

entre Etats constituants ou avec l'étranger, alors que les questions moins importantes ou d'intérêt purement local relèvent depuis toujours de la juridiction des Etats constituants. 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 constituants 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 constituants 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 2e 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

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 population[12] ». 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

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.

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.

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 Balkandali[13]), 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

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.

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 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 1998[14]).

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

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 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 315e 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.

Notes d'orientation

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[1].

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 »[2], et ce pour que de nouvelles formes de délits soient toujours couvertes par la Convention.

1. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
2. Paragraphe 36 du rapport explicatif.

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 8e 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.

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 1re 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 tés 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 9e réunion plénière du T-CY (4-5 juin 2013)

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 [3].

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 »[4], 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.

3. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
4. Paragraphe 36 du rapport explicatif.

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 (cyber-attaques). 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" »[5].

Des ordinateurs peuvent être reliés entre eux à des fins criminelles ou pour de bonnes causes[6]. 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.

---

5. 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).
6. 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.

Articles pertinents	Exemples
Article 2 – Accès illégal	La création et l'exploitation d'un botnet nécessitent un accès illégal à des systèmes informatiques[7]. 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[8].
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[9].

7. Voir également la note d'orientation n° 1 relative à la notion de «système informatique».
8. Voir la note d'orientation sur ce sujet.
9. 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
	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.

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 clémente 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 9e réunion plénière du T-CY (4-5 juin 2013)

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'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 technologies[10].

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 »[11], 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.

10. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
11. Paragraphe 36 du rapport explicatif.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE n° 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.

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.

Articles pertinents	Exemples
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 enfantine, 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. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par

Articles pertinents	Exemples
	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 9e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8e 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 techniques[12].

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 analogues[13].

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 »[14]. Cela vise à garantir que les nouvelles formes de criminalité seront toujours couvertes par la Convention.

12. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
13. Ces pratiques sont connues sous des appellations diverses : spear phishing ou « harponnage », SMiShing, pharming et vishing.
14. Paragraphe 36 du rapport explicatif.

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 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 (« keyloggers ») 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.

Phases	Articles de la Convention	Exemples
	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.
	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

Phases	Articles de la Convention	Exemples
		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 ».
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

Phases	Articles de la Convention	Exemples
		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 Parties à l'égard de l'usurpation d'identité soit trop clémente et ne permette 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

Phases	Articles de la Convention	Exemples
		« 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 9e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8e 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 technologies[15].

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 futures[16]. 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.

15. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
16. Paragraphe 36 du Rapport explicatif.

1. Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE n°185)

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). 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.
Article 7 – Falsification informatique	Les attaques contre les infrastructures d'information critiques peuvent introduire, altérer, effacer ou supprimer des données informatiques

Articles pertinents	Exemples
	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 entrainent 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 clémente 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

Articles pertinents	Exemples
	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 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 9e réunion plénière du T-CY (4-5 juin 2013)

Introduction

Lors de sa 8e 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 technologies[17].

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.

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[18]. 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.

17. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
18. Paragraphe 36 du Rapport explicatif.

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 »[19]. 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

19. www.oecd.org/internet/ieconomy/40724457.pdf.

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 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

Articles pertinents	Exemples
	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.
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.

Articles pertinents	Exemples
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.
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 clémente 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

Articles pertinents	Exemples
	et dissuasives compenant 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 données[20]

Introduction

Lors de sa 8e 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.[21]

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.[22]

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.

---

20. Adoptée lors de la 12e réunion plénière du T-CY (2-3 décembre 2014)
21. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
22. 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

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.

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.[23]

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.

23. La législation nationale peut toutefois limiter l'accès à des données publiquement disponibles ou leur utilisation par les services répressifs.

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.[24]

– 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.

Les autres situations ne sont ni autorisées ni exclues.[25]

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.[26]

---

24. Paragraphe 294 du rapport explicatif.

25. Paragraphe 293 du rapport explicatif. Voir aussi l'article 39.3 de la Convention de Budapest.

26. 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

Comme il a été souligné plus haut, les Parties à la convention sont supposées se faire mutuellement confiance et respecter

(Note 26 – Suite)

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,

les principes des droits de l'homme et de primauté du droit, conformément à l'article 15 de la Convention de Budapest.[27]

Les droits des individus et les intérêts des tiers doivent être pris en compte dans l'application de cette mesure.

(Note 26 – Suite)
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.

27. 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.

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 ».[28]

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 lumière de leur droit interne, des principes applicables de droit international ou des considérations liées aux relations internationales.

28. Paragraphe 293 du rapport explicatif de la Convention de Budapest

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.[29]

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.

---

29. 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 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.

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.[30]

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

30. Voir l'exemple donné dans le paragraphe 294 du rapport explicatif.

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 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 spams[31]

Introduction

Lors de sa 8e 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 technologies[32].

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 »[33], 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

31. Adoptée lors de la 12e réunion plénière du T-CY (2-3 décembre 2014)
32. Voir le mandat du T-CY (article 46 de la Convention de Budapest).
33. Paragraphe 36 du rapport explicatif.

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.

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 spam 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.
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.

Articles pertinents	Exemples
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.

Prems 027415 – 2015

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent.
Il comprend 47 États membres, dont les 28 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 de l'homme, la démocratie et l'Etat de droit. La Cour européenne des droits de l'homme contrôle la mise en oeuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE