Strasbourg, le 7 avril 2000
P:\cyber\ PROJET DE CONVENTION N°19.doc
11/04/00 21:00

Déclassifié – Version publique
PC-CY (2000) Projet n°19

COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS
(CDPC)

COMITE D'EXPERTS SUR LA CRIMINALITE DANS LE CYBER-ESPACE
(PC-CY)

Projet de Convention sur la cyber-criminalité
(Projet N° 19)

Etabli par le Secrétariat
Direction Générale I (Affaires Juridiques)

PROJET DE CONVENTION SUR LA CYBER-CRIMINALITÉ
(Projet N° 19)

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;

Estimant qu'une lutte bien menée contre la criminalité dans le cyberespace 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, l'intégrité et la disponibilité des systèmes informatiques, des réseaux et des données ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant la criminalisation de ces comportements, comme il est décrit 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, tout en garantissant un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits fondamentaux.

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, et notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8;

Rappelant la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur qui indique aux législateurs nationaux des principes directeurs pour définir certaines formes de criminalité informatique ainsi que la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de

l'information, qui préconise notamment la négociation d'un accord international pour réglementer la perquisition et la saisie transfrontières;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la justice à leur 21e conférence (Prague, juin 1997) qui recommande au Comité des Ministres de soutenir les activités menées par le Comité européen pour les problèmes criminels (CDPC) concernant la criminalité dans le cyberespace afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces, lors d'infractions informatiques;

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 Deuxième Sommet (Strasbourg, 10 - 11 octobre 1997) afin de chercher, sur la base des principes et des valeurs du Conseil de l'Europe, des réponses communes au développement des nouvelles technologies de l'information, sur la base des normes et des valeurs du Conseil de l'Europe;

Sont convenus de ce qui suit :

Chapitre I - Terminologie

Article 1 – Définitions[1]

Aux fins de la présente Convention, l'expression:

a. «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés qui assure, en exécution d'un programme, un traitement automatisé de données [ou d'autres fonctions][2];

b. «données informatiques» désigne:

- toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, ou

- un ensemble d'instructions de nature à faire en sorte qu'un système informatique exécute une fonction[3];

---

1 Le Groupe de rédaction est convenu à sa 10e réunion (février 2000) que la plupart des définitions figurant à l'article 1 devaient être insérées soit dans les parties pertinentes de la Convention soit dans le rapport explicatif, et a par conséquent retiré de cet article les définitions 1/e à 1/n. Les définitions restantes (1/a – 1/e) doivent être révisées par le GR.

2 Le rapport explicatif précisera que l'expression "système informatique" fait référence à la fonction du traitement des données et peut comprendre tout système basé sur une telle fonction, y compris les systèmes de télécommunication, et que "interconnecté" dans la définition englobe notamment les connexions radiophoniques et logiques. Le président a noté que dans les dispositions relatives à la compétence, le PC-CY devra décider de l'étendue de la compétence des Etats concernant les actes se produisant en tout ou en partie dans leur "système informatique".

3 Le concept de données informatiques inclut les programmes informatiques. Le Groupe de rédaction convient que le rapport explicatif devra préciser, soit à l'article 1, soit dans le cadre d'une autre

c. «fournisseur de service» désigne toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité d'envoyer ou de recevoir des communications électroniques;

d. «données relatives au trafic» désigne:

1. un code indiquant le numéro ou le compte d'un réseau, d'un équipement ou d'un particulier, ou un autre moyen d'identification similaire, transmis vers ou depuis tout point désigné dans la chaîne de communication;

2. l'heure, la date, la taille et la durée de la communication;

3. quel que soit le mode de communication (y compris mais non pas exclusivement les transmissions mobiles), toute information indiquant l'emplacement physique de l'origine ou de la destination d'une communication;

e. «données relatives à l'abonné» [4] désigne:

- toute information se trouvant en possession du fournisseur *de service* qui est nécessaire pour identifier et déterminer l'adresse physique d'un abonné, d'un utilisateur ou d'un titulaire de compte des services de communications d'un fournisseur *de service*, et

- toute information se rapportant à cet abonné, utilisateur ou titulaire de compte se trouvant en possession du fournisseur *de service*, qui concerne le numéro ou le compte d'un réseau, d'un équipement ou d'un particulier ou tout autre moyen d'identification similaire, services ou taxe ; l'emplacement physique de l'équipement [5], dès lors qu'il est connu et qu'il diffère des informations relatives à l'emplacement visées dans le cadre de la définition des données relatives au trafic;

---

disposition, qu'un «programme» est «un ensemble de données qui se prête à un traitement complémentaire».

4 Le rapport explicatif précisera que les «données relatives à l'abonné» ne comprennent pas celles concernant le trafic ni le contenu des communications.

5 Le rapport explicatif devra exclure sans équivoque la surveillance électronique, qui constitue une question juridique distincte.

Chapitre II - Mesures à prendre au niveau national

Section 1 - Droit pénal positif

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[6] *et* sans droit à tout ou partie d'un système informatique. Les Parties peuvent requérir que l'infraction soit commise soit en violation des mesures de sécurité soit dans une intention d'obtenir des données informatiques ou une autre intention délictueuse.

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[7], à destination, en provenance ou à l'intérieur d'un système informatique ainsi que des émissions électromagnétiques en provenance d'un système informatique transportant de telles données informatiques.

Article 4 - Atteinte à l'intégrité des données

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait d'endommager, d'effacer, de détériorer, d'altérer[8] ou de supprimer[9] des données informatiques, intentionnellement et sans droit[10].

---

6 Certains membres du Groupe de rédaction considèrent que "l'intention" peut également couvrir le "dol éventuel". Dans les pays de common law, cette notion pourrait être assimilée à celle de «recklessness», c.-à-d. au fait qu'une personne est consciente du risque de voir se produire un certain résultat et l'accepte sciemment. Le Groupe de rédaction a considéré que l'interprétation de "l'intention" devait être laissée aux droits nationaux, mais qu'elle ne devrait pas exclure, dans la mesure du possible, le «dol éventuel».

7 Le Groupe de rédaction a établi le principe, lors de sa 9e réunion (janvier 2000), que l'expression "non-publique" se réfère au moyen de transmission (communication) et pas forcément aux données qui sont transmises. Il a convenu que l'expression serait provisoirement maintenue dans le texte tout en essayant de trouver une meilleure expression.

8 Le Groupe de rédaction est convenu à sa 8e réunion (novembre 1999) que le rapport explicatif devrait préciser que la notion d"altération" devait également couvrir le fait de manipuler les données relatives au trafic ("spoofing").

9 Pour le Groupe de rédaction, l'expression "supprimer des données" recouvre deux acceptions généralement admises: 1) effacer des données de telle sorte qu'elles cessent physiquement

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[11] intentionnelle et sans droit au fonctionnement d'un système informatique, par l'introduction, le transfert, l'endommagement, l'effacement, la détérioration, l'altération et la suppression de données informatiques.

6. Dispositifs illégaux

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'il est commis 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,

   1) d'un dispositif, y compris un programme informatique, [spécialement] [principalement] conçu [en particulier] pour permettre la commission de l'une des infractions établies conformément aux articles 2 – 5 ci-dessus ;
   2) 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

   dans l'intention qu'il soit utilisé afin de commettre l'une des infractions visées par les articles 2 – 5 ;

b) La possession d'un article visé aux paragraphes (a) (1) et (2) ci-dessus dans l'intention qu'il soit utilisé afin de commettre l'une des infractions visées par les articles 2 – 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces articles soit détenu pour que la responsabilité soit engagée.

---

d'exister; 2) "rendre inaccessible", c'est-à-dire empêcher quelqu'un d'y accéder tout en les conservant. Etant donné que cette seconde acception désigne le fait de "rendre inaccessible", qui était traité séparément dans les versions précédentes de cet article, cet élément a été supprimé, étant entendu qu'une note en fera mention dans le rapport explicatif.

10 Une délégation a fait remarquer qu'elle souhaiterait que des éléments supplémentaires soient inclus dans le texte (dommage ou préjudice sérieux) afin de pouvoir rendre l'infraction passible d'extradition.

11 Lors de la 9e réunion du Groupe de rédaction (janvier 2000), le terme "serious" a été rajouté après le mot "hindering" dans la version anglaise du texte afin d'éviter le risque d'une incrimination excessive et de mieux rendre le sens du terme "entrave" dans la version française.

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 puissent être prises en compte ou utilisées à des fins légales comme si elles étaient authentiques[12], indépendamment du fait qu'elles sont ou non directement lisibles et intelligibles. Une Partie peut exiger en droit interne une intention frauduleuse ou une intention pernicieuse similaire pour que la responsabilité 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 de causer intentionnellement et sans droit un préjudice patrimonial à autrui par:

a) l'introduction, l'altération, l'effacement ou la suppression de données informatiques,
b) toute forme d'atteinte au fonctionnement [d'un programme ou] d'un système informatique[s],

dans l'intention 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 sans droit[13] et intentionnellement:

   a. offrir[14], distribuer, transmettre ou rendre disponible [par tout autre moyen] de la pornographie enfantine par le biais d'un système informatique ;
   b. Produire de la pornographie enfantine en vue de la diffuser par le biais d'un système informatique[15];

---

12 Le rapport explicatif indiquera que le terme "authentique" se réfère à l'émetteur des données, sans tenir compte du caractère véridique ou faux du contenu de données.

13 Le rapport explicatif indiquera que l'expression "sans droit" inclut des exceptions et excuses légales, des faits justificatifs ou d'autres principes similaires qui absolvent une personne de la responsabilité pénale dans certaines circonstances.

14 Le Groupe de rédaction est convenu à sa 8ème réunion (novembre 1999) que le rapport explicatif devra indiquer que le terme "offrir" comprend également le fait de donner des informations concernant les hyperliens vers des sites pédophiles.

c. posséder de la pornographie enfantine dans un système informatique ou sur un support[16] de données.

2. Aux fins du paragraphe 1 ci-dessus, la «pornographie enfantine» comprend toute matière pornographique[17] représentant de manière visuelle :

a. un mineur se livrant à un comportement sexuellement explicite[18];
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» est à définir par chaque État membre, mais désigne en tout état de cause toute personne âgée de moins de [quatorze][19] ans.

Titre 4 - Infractions liées à la propriété intellectuelle et infractions connexes

Article 10 - Infractions liées à la propriété intellectuelle et infractions connexes

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, la reproduction et la diffusion, par le moyen d'un système informatique, d'oeuvres protégées au titre du droit d'auteur, tel que défini par le droit interne de cette Partie [conformément à la Convention de Berne sur la protection des œuvres littéraires et artistiques, l'accord ADPIC et le Traité de l'OMPI sur les droits d'auteur], lorsque ces actes sont commis intentionnellement, à l'échelle commerciale, sans droit.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, la reproduction et la diffusion ou d'autres actes similaires, par le moyen d'un système

---

15 Le rapport explicatif devra préciser que cette disposition ne vise nullement à limiter l'incrimination de la diffusion etc. de la pornograpie enfantine aux cas où il est fait usage d'un système informatique, mais que la Convention établit ainsi une norme minimum, les Etats étant libres d'aller au delà.

16 Certaines délégations ont exprimé le souhait de pouvoir repenser leur positions quant cette disposition et d'en consulter davantage avec leurs autorités nationales. Néanmoins, nombre de délégations considéraient qu'une telle disposition était nécessaire pour prévenir des actes d'abus sexuel lors de la production du matériel pédophile.

17 Le rapport explicatif devra préciser que l'expression "matière pornographique" doit être interprétée en conformité avec les normes de droit interne concernant la classification du matériel comme "obscène", incompatible avec les moeurs publiques ou ayant autrement un effet pervers.

18 Le rapport explicatif devra préciser que l'expression «comportement sexuellement explicite» désigne l'un ou l'autre des comportements réels ou simulés : 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 ; b) masturbation ; d) violences sado-masochistes ; e) exhibition lascive des parties génitales ou de la région pubienne d'un mineur.

19 Plusieurs alternatives ont été soulevées: 14, 16 et 18 ans

informatique, d'oeuvres, [d'articles] ou de créations équivalentes protégées au titre des droits voisins, tel que défini par le droit interne de cette Partie [conformément au Traité de l'OMPI sur interprétations, exécutions et phonogrammes], lorsque ces actes sont commis intentionnellement, à l'échelle commerciale, sans droit.

Titre 5 – D'autres formes de responsabilité et sanctions

Article 11 - Tentative et complicité

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:

(a) toute tentative de commission de l'une des infractions établies en conformité avec les articles […][20]
(b) toute complicité[21] dans la commission de l'une des infractions établies en conformité avec les articles 2 – 10 ci-dessus.

Article 12 - Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions établies en vertu 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, sur les bases suivantes:

- un pouvoir de représentation de la personne morale; ou
- une autorité pour prendre des décisions au nom de la personne morale; ou
- une autorité pour exercer un contrôle au sein de la personne morale;
- ainsi que la participation d'une telle personne physique en qualité de complice ou d'instigatrice, aux termes de l'article 11, à la commission des infractions visées ci-dessus.

2 Abstraction faite des cas déjà prévus au paragraphe 1, chaque Partie prend les mesures nécessaires pour s'assurer qu'une personne morale puisse être tenue

---

20 Le Plénier est convenu que lorsque la liste des infractions sera finalisée dans le projet de Convention, cette disposition sur «la tentative» sera rediscutée afin de décider à quelles infractions elle devra s'appliquer. Les délégations ont déjà exprimé leurs préoccupations concernant l'application de la disposition sur la tentative à l'accès illégal, défini par [l'article 2(1)], ainsi qu'aux infractions relatives à la propriété intellectuelle et aux infractions connexes, définies à [l'article 4] (car la tentative n'est pas couverte par l'accord ADPIC).

21 Le Plénier est convenu que le rapport explicatif devrait clarifier la nécessité d'intention double pour incriminer la complicité, c.-à.-d. que l'intention doit couvrir à la fois la complicité et l'infraction principale. Le rapport explicatif devra spécifier aussi que «toute complicité» doit être interprété au sens large, englobant, notamment, les instigateurs et les auxiliaires.

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 visées au paragraphe 1 pour le compte de ladite personne morale par une personne physique soumise à son autorité.

3 La responsabilité de la personne morale en vertu des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs, instigatrices ou complices des infractions visées au paragraphe 1.

Article 13 - Sanctions et mesures

1. Chaque Partie prend les mesures législatives et autres qui se révèlent nécessaires pour faire en sorte que les infractions pénales établies en vertu des articles 2 - 11 soient passibles de sanctions et de mesures effectives, proportionnées et dissuasives. En particulier, chaque Partie s'assure que les infractions établies conformément aux articles [..][22] ainsi que celles visées à l'article 21, paragraphe 1, lorsqu'elles sont commises par des personnes physiques, sont passibles de peines privatives de liberté pouvant donner lieu à extradition.

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

Section 2 – Droit de procédure

Article 14 - Perquisition et saisie des 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 et aux données informatiques qui y sont stockées ; ou

    b) à un support permettant de stocker des données informatiques

    sur [son territoire ou en un autre lieu relevant de sa souveraineté][23], pour les besoins d'enquêtes ou de procédures pénales.

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

---

22 L'on devra continuer la réflexion quant aux infractions à inclure dans cette disposition lorsque la liste des infractions pénales sera établie. En l'état actuel des choses, de nombreux Etats ne considèrent pas l'accès illégal comme une infraction pouvant donner lieu à une extradition ; de même, la tentative n'est pas toujours passible d'extradition.

23 Lors de sa 7e réunion (mars 2000), le Comité plénier a invité le Groupe de rédaction à trouver une formule alternative pour décrire le concept de la "territorialité".

partie de celui-ci, en recourant aux mesures visées 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, sur son territoire ou en un autre lieu relevant de sa souveraineté, 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 un moyen d'accès similaire à l'autre système.

3. [S'il s'avère que l'accès au système informatique ou à une partie de celui-ci ou à des données informatiques dont l'accès est autorisé en vertu du paragraphe 1 ou du paragraphe 2 se fait par inadvertance dans la juridiction d'une autre Partie, les autorités compétentes de la Partie menant l'enquête procèdent conformément aux dispositions de l'article […]][24]

4. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à acquérir d'une façon similaire les données informatiques auxquelles l'accès a été obtenu en vertu des paragraphes 1 ou 2, en vue de leur utilisation éventuelle dans des enquêtes et procédures pénales. Ces mesures incluent les prérogatives suivantes :

   a) saisir ou acquérir d'une façon similaire un système informatique ou une partie de celui-ci ou un support permettant de stocker des données informatiques ;
   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.

5. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes, pour les besoins d'enquêtes et de procédures pénales, à enjoindre 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 4.

6. Lorsque des mesures visées par les paragraphes 1 et 2 ont été prises à l'égard d'un système informatique ou d'une partie de celui-ci, ou des données informatiques qui y sont stockées, la personne responsable[25] du système informatique doit, dès que cela est raisonnablement possible, être dûment informée des mesures exécutées.

---

24 Le Groupe de rédaction n'a pas examiné cette disposition lors de sa 10e réunion (février 2000), car elle est étroitement liée à la disposition sur les perquisitions transfrontalières.

25 Le Groupe de rédaction a décidé lors de sa 10e réunion (février 2000) d'employer ce terme et de préciser dans le rapport explicatif qu'il renvoie aux personnes qui exercent un contrôle (physique) effectif sur l'ordinateur (ou le système informatique). Cela inclut en principe le propriétaire des lieux où se trouve l'ordinateur ou le propriétaire/utilisateur de l'ordinateur.

7. Les prérogatives et les mesures visées par le présent article sont subordonnées aux conditions et garanties prévues par le droit interne.

Article 15 - Injonction de produire

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à enjoindre à une personne présente sur son territoire ou en un autre lieu relevant de sa souveraineté de fournir des données informatiques spécifiées qui sont sous le contrôle de cette personne et sont stockées dans un système informatique [ou un support [26] permettant de stocker des données informatiques], sous la forme requise par ces autorités, pour les besoins d'enquêtes et de procédures pénales.

2. La prérogative visée par le paragraphe 1 du présent article est subordonnée aux conditions et garanties prévues par le droit interne.

Article 16 – Conservation rapide de données stockées dans un système informatique

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'obtenir d'une autre façon, pour les besoins d'enquêtes ou de procédures pénales, la conservation rapide de données stockées au moyen d'un système informatique, du moins lorsqu'il y a des raisons de penser que celles-ci sont soumises à une période de conservation limitée ou sont, à d'autres titres, particulièrement sensibles aux risques de perte ou de modification.

2. Lorsqu'une Partie applique le paragraphe 1 ci-dessus en enjoignant une personne de conserver des données stockées spécifiées se trouvant en la possession ou sous le contrôle de celle-ci, ladite Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité de ces données pendant la durée exigée, conformément aux dispositions du droit interne.

3. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger la personne à qui s'adressent les procédures de conservation visées par le présent article de garder le secret sur la mise en oeuvre desdites procédures pendant une durée autorisée par le droit interne.

4. Les prérogatives et les procédures visées par le présent article sont subordonnées aux conditions et garanties prévues par le droit interne.

---

[26] Lors de sa 7e réunion (mars 2000), le Comité plénier a invité le Groupe de rédaction à trouver une formule alternative pour remplacer le terme anglais "medium" dans la version anglaise.

Article 17 - Conservation et divulgation rapides de données relatives au trafic

1. Pour mettre en oeuvre les procédures visées par l'article 16 en vue de la conservation de données relatives au trafic concernant une communication spécifique, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour :

   a) veiller à la conservation rapide de ces données relatives au trafic, indépendamment de la question de savoir si un seul ou plusieurs fournisseurs de service ont participé à la transmission de cette communication ; et

   b) 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, aux fins d'identification des fournisseurs de service et de la voie par laquelle la communication a été transmise.

2. Les prérogatives et les procédures visées par le présent article sont subordonnées aux conditions et garanties prévues par le droit interne.

Article 18 – Interception
(en cours de rédaction)

Section 3 - Compétence

Article 19 - Compétence

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

a [en tout ou en partie] sur son territoire, à bord d'un navire, d'un aéronef ou d'un satellite[27] battant son pavillon ou étant immatriculé dans cette Partie;

b 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 Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, dans une déclaration adressée au Secrétaire Général du Conseil de l'Europe, préciser qu'il se réserve le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou conditions spécifiques, les règles de compétence définies au paragraphe 1b du présent article ou une partie quelconque de ces paragraphes.

3. Lorsqu'une Partie a fait usage de la possibilité de réserve prévue au paragraphe 2 du présent article, elle adopte les mesures qui se révèlent nécessaires pour établir sa compétence relativement à toute infraction pénale mentionnée à l'article 21, 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. Dans la présente Convention, rien ne saurait être interprété comme excluant l'exercice par une Partie de sa compétence, établie conformément à son droit interne.

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

---

27 Des clarifications supplémentaires devront être apportées concernant l'inclusion des satellites, en particulier quant à la question de savoir si un Etat reponsable d'un satellite (ou partage cette responsabilité avec d'autres Etats) devrait, en vertu de cette disposition, établir sa compétence concernant une infraction dont le seul lien avec cet Etat est que les données impliquées par l'infraction ont transité par le satellite. D'autres intruments internationaux devront être pris en considération pour voir comment la compétence des Etats est régie en matière de satellites.

Chapitre III – Coopération internationale

Article 20 - Principes généraux relatifs à la coopération internationale

Les Parties coopèrent, 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 de leur droit national, dans la mesure la plus large possible les unes avec les autres, aux fins d'investigations et de procédures concernant les infractions pénales liées à des systèmes et données informatiques ou afin de recueillir des preuves électroniques se rapportant à une infraction pénale.

Article 21 - Extradition

1. Les infractions pénales définies conformément aux articles 3 – 5 et 7 – 11 de la présente Convention seront considérés comme incluses à titre d'infractions pouvant donner lieu à l'extradition dans tout traité d'extradition existant entre les ou des Parties. Les Parties s'engagent à inclure ces infractions à titre d'infractions pouvant donner lieu à l'extradition dans tout traité d'extradition signé à l'avenir entre elle ou certaines d'entre elles. S'agissant des infractions pénales définies à l'article 2, les critères suivants peuvent être requis pour que l'infraction soit considérée comme pouvant donner lieu à l'extradition :

   - [l'accès sans droit doit avoir été pratiqué dans l'intention de violer la confidentialité des données ou de porter atteinte à l'intégrité ou à la disponibilité de données ou d'un système informatique, ou]

   - [l'accès sans droit doit avoir porté atteinte à l'intégrité ou à la disponibilité de données ou d'un système informatique]

2. Lorsqu'une Partie conditionne l'extradition a 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.

3. 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.

4. L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, s'agissant aussi des motifs pour lesquels la Partie requise peut refuser l'extradition.

5. 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 ses autorités compétentes

aux fins de poursuites, à moins qu'il en soit convenu autrement avec la Partie requérante, et rendra compte en temps utile de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision de la même manière que pour toute autre infraction de nature comparable conformément à la législation de leur Etat.

6. (a) En l'absence de traité, chaque Partie communiquera 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. [La désignation d'une autorité n'exclut pas la possibilité d'utiliser la voie diplomatique.][28]

(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.

Article 22 - Entraide

1. Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations et de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir des preuves électroniques se rapportant à une infraction pénale.

2. Chaque Partie adopte également les mesures législatives ou autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 24 - 29.

3. Aux fins de la coopération prévue aux articles 24 - 29, dans les cas d'urgence, chaque Partie accuse réception des demandes d'entraide et y répond par des moyens rapides de communication, tels que le [téléphone], la télécopie ou le courrier électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification, avec confirmation officielle si l'Etat requis l'exige.

4. Sauf disposition contraire expressément prévue dans les articles 24 – 29, 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[29].

---

28 Cette disposition s'applique uniquement dans le cas où il n'existe pas de traité d'extradition entre les Parties. Lorsqu'il existe entre les Parties concernées un traité biltéral ou multilatéral d'extradition (comme la Convention européenne d'extradition de 1957), les Parties savent à qui adresser leurs demandes d'extradition et d'arrestation provisoire et, dans ce cas, cette obligation d'enregistrement un peu pesante n'a pas de raison d'être. Le texte entre crochets régissant le recours à la voie diplomatique est calqué sur l'article 5 du deuxième protocole additionnel à la Convention européenne d'extradition.

29 N.B. Le Groupe de rédaction n'est pas pour le moment parvenu à s'entendre sur cette disposition.

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, en relation avec laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, sans qu'il y ait lieu de se demander si ledit droit interne classe l'infraction dans la même catégorie d'infractions ou la désigne par la même terminologie que le droit de la Partie requérante.

Article 23 - Procédures applicables en matière de demande d'entraide

1. En l'absence d'un traité ou d'un accord d'entraide fondé sur une législation uniforme ou réciproque en vigueur entre la Partie requérante et la Partie requise, ou lorsque les Parties concernées ne se sont pas dotées de lois nationales permettant l'entraide,[30] les dispositions des paragraphes 2 à 10 du présent article s'appliquent. Les dispositions du présent article ne s'appliquent pas lorsqu'un accord ou une législation[31] de ce type existe, à moins que les Parties concernées 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 constitue et met à jour un registre des autorités centrales désignées par les Parties. Chaque Partie s'assure que les indications figurant sur ce registre sont à tout moment correctes.

3. Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorqu'elle est incompatible avec la législation de la Partie requise.[32]

4. Outre les conditions ou motifs de refus prévus à l'article 22(4), l'entraide peut être refusée par la Partie requise si celle-ci estime que le fait d'accéder à la

---

30 Le Groupe de rédaction peut souhaiter examiner encore si le fait de conserver le texte entre parenthèses risque de rendre le reste de l'article inapplicable dans pratiquement tous les cas.

31 Voir note précédente.

32 La note explicative devrait préciser que le seul fait que cette procédure ne soit pas prévue dans le droit interne de la partie requise ne constitue pas un motif suffisant pour refuser de l'appliquer.

demande porterait 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 des mesures visées par une demande si elle estime que celles-ci risqueraient de porter préjudice à des enquêtes, des poursuites ou toute autre procédure liée menées 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 y être fait droit partiellement ou sous réserve de 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 motive son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de toute raison rendant impossible l'exécution de l'entraide ou susceptible de la retarder de manière significative.

8. (a) Sans préjudice de ses propres enquêtes ou procédures, une Partie peut, dans les limites de son droit interne et sans demande préalable, transmettre à une autre partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que la divulgation de ces informations est susceptible d'aider la Partie bénéficiaire à ouvrir ou à poursuivre ses enquêtes ou procédures concernant une infraction pénale établie en vertu de la présente convention ou d'entraîner une demande de cette Partie au sens du présent chapitre.

(b) Avant de transmettre ces informations, la Partie qui les détient peut demander qu'elles restent confidentielles ou soient utilisées sous certaines conditions. Si la Partie bénéficiaire ne peut accéder à cette demande, elle le notifie à l'autre Partie qui décide alors s'il convient néanmoins de les communiquer. Lorsqu'une Partie accepte de recevoir des informations sous certaines conditions, elle est liée par elles.

9. (a) La Partie requérante peut exiger de la Partie requise qu'elle conserve un caractère confidentiel à l'existence et à la teneur de toute demande faite en application du présent chapitre, sauf dans la mesure nécessaire pour y faire droit. Si la Partie requise ne peut se conformer à cette condition de confidentialité, elle en informe la Partie requérante dans les plus brefs délais; celle-ci décide alors s'il convient néanmoins de faire droit à la demande.

(b) La Partie requérante peut demander que la Partie requise recherche son consentement avant d'utiliser le fond même de la demande ou les informations obtenues pour faire droit à la demande, à des fins autres que celles pour lesquelles elles ont été obtenues ou pour des enquêtes pénales et des procédures apparentées. Si la Partie requise ne peut se conformer à la demande, elle en informe aussitôt la Partie requérante qui décide alors s'il convient néanmoins de donner suite à sa demande.

(c) La Partie requise peut demander que la Partie requérante recherche son consentement avant de transmettre ou d'utiliser les informations demandées à des fins d'enquêtes ou de procédures autres que celles spécifiées dans la demande. Si la Partie requérante accepte les informations sous cette condition, elle est tenue de s'y conformer. Si elle ne peut s'y conformer, elle en informe aussitôt la Partie requise qui décide s'il convient néanmoins de transmettre les informations.

10. a. En cas d'urgence, les autorités judiciaires, y compris le ministère public, de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. En pareil cas, copie doit en être simultanément envoyée à l'autorité centrale de la Partie requise par l'intermédiaire de l'autorité centrale de la Partie requérante;

b. toute demande ou communication effectuée en application du présent paragraphe peut être transmise par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol);

c. lorsqu'une demande est formulée en application de l'alinéa (a) du présent article et que 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 et 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 24 - Mesures provisoires : conservation rapide de données informatiques stockées

1. Une Partie peut demander à une autre Partie d'ordonner ou d'obtenir 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 [ou en un autre lieu relevant de sa souveraineté], 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'acquisition par un moyen similaire, ou de la communication desdites données.

2. Une demande de conservation déposée en vertu du paragraphe 1 doit comporter les éléments suivants :
   a) l'autorité qui demande la conservation ;
   b) l'infraction faisant l'objet de l'enquête et un bref exposé des faits qui s'y rattachent ;

c) les données stockées à conserver et la nature de leur lien avec l'infraction ;
d) la nécessité de la mesure de conservation ;
e) 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'acquisition par un moyen similaire, ou de la communication desdites données .

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 []. En répondant à une telle demande, la double incrimination n'est pas requise comme une condition préalable à la conservation, mais elle peut être une condition à la communication des données à la Partie requérante[33].

4. Une demande de conservation telle que prévue au paragraphe 2 peut être refusée uniquement si la Partie requise estime que faire droit à la demande porterait atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5. Lorsque la Partie requise estime que la conservation simple ne suffira pas pour garantir la disponibilité future des données, 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 de faire droit à la demande.

6. Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins 40 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 communication des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant la prise d'une décision concernant la demande.

Article 25 – Communication rapide de données conservées relatives au trafic

1. Lorsqu'en faisant droit à une demande faite en vertu de l'article 24 en vue de la conservation de données relatives au trafic concernant une communication spécifique, la Partie requise découvre qu'un fournisseur de service dans un Etat tiers a participé à la transmission de cette communication, la Partie requise communique rapidement à la Partie requérante une quantité suffisante de données relatives au trafic aux fins d'identification du fournisseur de service et de la voie par laquelle la communication a été transmise.

2. La communication de données relatives au trafic en vertu du paragraphe 1 ne peut être refusée que si la Partie requise estime que le fait d'accéder à la

---

[33] Le Comité plénier est convenu lors de sa 7e réunion (mars 2000) qu'une réflexion supplémentaire serait nécessaire concernant ce sujet, car certaines délégations ont exprimé des réserves quant à la possibilité d'abandonner la condition de double incrimination.

demande porterait atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Article 26 - Entraide [] concernant l'accès aux données stockées[34]

[1. Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'acquérir de façon similaire, ou de communiquer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie ou en un autre lieu relevant de sa souveraineté, y compris les données conservées conformément à l'article 24.

2. Dès réception d'une demande visée au paragraphe 1, la Partie requise devra satisfaire à la demande aussi rapidement que possible, de l'une des manières suivantes:

a) lorsque cela est autorisé par son droit interne, en ratifiant ou en endossant toute autorisation judiciaire ou autre autorisation légale accordée dans l'État requérant pour perquisitionner ou saisir les données, en procédant à la perquisition et/ou à la saisie et en communiquant toute donnée saisie à l'État requérant, conformément aux traités d'entraide judiciaire dont elle est Partie ou à ses lois en la matière; ou

b) en répondant à la demande et en communiquant toute donnée saisie, conformément aux traités d'entraide judiciaire dont elle est Partie ou à ses lois en la matière;

c) en appliquant toute autre méthode d'entraide autorisée par son droit interne.

Article 27 – Accès transfrontalier à des données stockées ne nécessitant pas l'entraide judiciaire

[Nonobstant les dispositions de la présente section, une Partie peut, lorsqu'elle agit conformément à son droit interne [sans obtenir l'autorisation d'un autre Etat ou lui adresser une notification] :

a) obtenir accès à des informations accessibles au public [source ouverte], quelle que soit la localisation géographique de ces données ;

b) obtenir accès ou recevoir de données stockées situées dans un autre État, si la Partie [était en contact avec une personne relevant de la juridiction et] agit conformément au consentement légal et volontaire d'une personne de l'État qui est légalement autorisée à permettre à la Partie d'accéder à ces données ou de les lui communiquer.][35]

---

34 Le chapeau a été modifié pour calquer la terminologie du principe du G8. Le texte n'est pas la proposition d'origine des USA, mais l'ancien Article 16 [8bis] tel qu'amendé par M. Piragoff et révisé par le GR lors de sa 7ème réunion (sept. 1999), cf. document PC-CY DG7 Misc 4 rev 1.

35 Ce paragraphe part de l'hypothèse que l'Etat qui accède aux données limitera son contact aux personnes se trouvant sur son territoire (même si ces personnes peuvent avoir besoin de contacter

Article 28 - Interception
[en cours de rédaction]

Article 29 - Réseau 24/7

1. Chaque Partie désigne un point de contact joignable 24 heures sur 24, sept jours sur sept, afin de fournir une assistance immédiate aux fins d'investigations concernant les infractions pénales liées à des systèmes et données informatiques ou afin de recueillir des preuves électroniques se rapportant à une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

(1) apport de conseils techniques;

(2) conservation des données conformément aux articles 24 et 25 ; et

(3) recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2. *a*. Le point de contact d'une Partie pourra 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 V - Suivi

Chapitre VI - Clauses finales

---

d'autres personnes sur d'autres territoires afin d'obtenir un tel consentement ou autorisation). Ceci pourrait être rajouté en incluant la partie entre crochets ou être expliqué dans le rapport explicatif.