COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Version 28 mai 2021

T-CY (2020)7

T-CY(2020)7_FR_PDP_Protocol_v3t (approuvé par le TCY)

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

Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Projet de Protocole version 3

Approuvé par le T-CY lors de sa 24ème Plénière du T-CY (28 mai 2021)

Contenu

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Préambule

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

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

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

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

Compte tenu également de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) telle qu'amendée par son Protocole d'amendement (STCE n° 223), ouvert à la signature à Strasbourg le 10 octobre 2018, et auquel tout État peut être invité à adhérer;

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

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

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

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

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

Entendant donc renforcer encore la coopération concernant la cybercriminalité et le recueil de preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques grâce à des outils supplémentaires relevant d'une entraide plus efficiente

et d'autres formes de coopération entre autorités compétentes; de la coopération en situation urgente; et de la coopération directe entre autorités compétentes et fournisseurs de services et autres entités qui possèdent ou contrôlent les informations pertinentes;

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

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

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

Sont convenus de ce qui suit:

Chapitre I - Dispositions communes

Article 1 – But

Le présent Protocole a pour but de compléter:

a. la Convention entre les Parties au présent Protocole; et

b. le Premier Protocole entre les Parties au présent Protocole qui sont aussi parties au Premier Protocole.

Article 2 – Champ d'application

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

   a. pour ce qui concerne les Parties à la Convention qui sont parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques, ainsi qu'au recueil de preuves d'une infraction pénale sous forme électronique; et

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

2. Chaque Partie adopte les mesures législatives ou autres pouvant se révéler nécessaires pour s'acquitter des obligations entérinées dans le présent Protocole.

Article 3 – Définitions

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

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

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

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

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

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

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

Article 4 – Langue

1 Les demandes, les injonctions et les renseignements qui les accompagnent présentés à une Partie doivent être rédigés dans une langue acceptable pour la Partie requise ou la Partie à laquelle ils sont notifiés en vertu de l'article 7, paragraphe 5, ou être accompagnés d'une traduction dans cette langue.

2 Les injonctions visées à l'article 7 et les demandes visées à l'article 6 et toute information qui les accompagne seront:

   a. rédigés dans une langue de l'autre Partie dans laquelle le prestataire de services ou l'entité les accepte dans le cadre d'une procédure nationale comparable;

   b. rédigés dans une autre langue acceptable pour le fournisseur de services ou l'entité; ou

   c. accompagnés d'une traduction dans l'une des langues visées aux paragraphes 2.a ou 2.b.

Chapitre II - Mesures de coopération renforcée

Section 1 – Principes généraux applicables au chapitre II

Article 5 – Principes généraux applicables au chapitre II

1. Conformément aux dispositions du présent chapitre, les Parties s'assurent la coopération mutuelle la plus large possible.

2. La section 2 de ce chapitre se compose des articles 6 et 7. Elle prévoit des procédures renforçant la coopération directe avec les fournisseurs et les entités sur le territoire d'une autre Partie. La section 2 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées.

3. La section 3 du présent chapitre est constituée des articles 8 et 9. Elle prévoit des procédures visant à renforcer la coopération internationale entre les autorités pour la divulgation de données informatiques stockées. La section 3 s'applique, qu'il existe ou non un traité ou un arrangement d'entraide reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.

4. La section 4 du présent chapitre est constituée de l'article 10. Elle prévoit des procédures relatives à l'entraide d'urgence. La section 4 s'applique qu'il existe ou non un traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise.

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

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

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

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

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

1. Chaque Partie adopte les mesures législatives et autres nécessaires pour habiliter ses autorités compétentes aux fins d'enquêtes ou procédures pénales spécifiques, à émettre auprès d'une entité fournissant des services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie une demande d'informations en la possession ou sous le contrôle de l'entité en vue d'identifier ou de contacter la personne ayant enregistré un nom de domaine.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à une entité située sur son territoire de divulguer de telles informations en réponse à une demande introduite en vertu du paragraphe 1, sous réserve des conditions raisonnables prévues par le droit interne.

3. La demande visée au paragraphe 1 contient:

   a. la date d'émission de la requête, l'identité et les coordonnées de l'autorité émettrice compétente;
   b. le nom de domaine pour lequel les informations sont demandées et une liste détaillée des informations demandées, y compris les éléments de données particuliers;
   c. une mention déclarant que la demande est émise en vertu du présent Protocole et que l'information est nécessaire du fait de la pertinence qu'elle revêt pour une enquête ou procédure pénale spécifique; et qu'elle ne sera utilisée que dans le cadre de cette enquête ou procédure pénale; et
   d. le délai et le moyen de divulgation de ces informations et toutes autres instructions procédurales spéciales.

4. Si l'entité le juge acceptable, une Partie peut présenter une demande au titre du paragraphe 1 sous forme électronique. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.

5. Si une entité visée au paragraphe 1 ne coopère pas, la Partie requérante peut lui demander de motiver la non-divulgation des informations demandées. La Partie requérante peut envisager une consultation avec la Partie sur le territoire de laquelle l'entité est située en vue de déterminer les mesures disponibles pour obtenir les informations.

6. Chaque Partie, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, communique au Secrétaire Général du Conseil de l'Europe l'autorité désignée aux fins de consultation en vertu du paragraphe 5.

7. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 6. Chaque Partie veille à ce que les informations qu'elle a fournies pour le registre soient exactes à tout moment.

Article 7 – Divulgation directe de données relatives aux abonnés

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à adresser directement à un fournisseur de services sur le territoire d'une autre Partie une injonction de produire des données spécifiées et stockées relatives à des abonnés, en la possession ou sous le contrôle du fournisseur, lorsque ces informations sont nécessaires à des enquêtes ou des procédures pénales spécifiques menées par la Partie émettrice.

2. a. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour qu'un fournisseur de services sur son territoire communique des données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1.

   b. Au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut – en ce qui concerne les injonctions adressées aux fournisseurs de services sur son territoire – faire la déclaration suivante: « l'injonction adressée en application de l'article 7, paragraphe 1, doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une autre forme de supervision indépendante. »

3. L'injonction, adressée en application du paragraphe 1, doit comprendre:

   a. l'autorité émettrice et la date d'émission;
   b. une déclaration indiquant que l'injonction est émise en vertu du présent Protocole;
   c. le nom et l'adresse du ou des fournisseurs de services visés;
   d. la ou les infractions faisant l'objet de l'enquête ou de la procédure pénale;
   e. l'autorité qui sollicite les données spécifiques relatives aux abonnés, s'il ne s'agit pas de l'autorité émettrice; et
   f. les données spécifiques relatives aux abonnés qui sont demandées, au moyen d'une description détaillée.

4. L'injonction adressée en application du paragraphe 1 doit être accompagnée des informations complémentaires suivantes:

   a. le fondement juridique interne qui habilite l'autorité à adresser une injonction;
   b. la mention des dispositions juridiques et des sanctions applicables à l'infraction qui est à l'origine d'une enquête ou de poursuites;
   c. les coordonnées de l'autorité à laquelle le fournisseur de services doit communiquer les données relatives aux abonnés, à laquelle il peut demander de plus amples informations ou adresser toute autre réponse;
   d. le délai et le mode de communication des données relatives aux abonnés;
   e. l'indication d'une éventuelle demande de conservation des données précédemment formulée, en précisant la date de conservation et tout numéro de référence applicable;
   f. tout type d'instructions spéciales en matière de procédure; et
   g. le cas échéant, une déclaration selon laquelle la notification simultanée a été faite conformément au paragraphe 5; et
   h. toute autre information qui pourrait aider à obtenir la divulgation des données relatives aux abonnés.

5. a. Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, notifier au Secrétaire Général du Conseil de l'Europe qu'elle exige,

lorsqu'une injonction est adressée en application du paragraphe 1 à un fournisseur de services sur son territoire, dans chaque cas ou dans certaines circonstances déterminées, la communication simultanée de l'injonction, des informations complémentaires et d'un résumé des faits relatifs à l'enquête ou à la procédure.

b. Qu'une Partie exige ou non la communication d'informations prévue au paragraphe 5.a, elle peut, dans certaines circonstances déterminées, demander au fournisseur de services de consulter les autorités de la Partie avant de divulguer les données demandées.

c. Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b peuvent, dans les plus brefs délais, enjoindre au fournisseur de services de ne pas divulguer les données demandées, si :

   i. cette divulgation risque de porter préjudice à des enquêtes ou procédures pénales menées sur le territoire de cette Partie; ou
   ii. les conditions ou les motifs de refus visés aux articles 25, paragraphe 4 et 27, paragraphe 4, de la Convention s'appliquent parce que les données relatives aux abonnés ont fait l'objet d'une demande d'entraide.

d. Les autorités informées en application du paragraphe 5.a ou consultées en application du paragraphe 5.b

   i. peuvent demander des informations complémentaires à l'autorité visée au paragraphe 4.c aux fins de l'application du paragraphe 5.c et ne les divulgueront pas au fournisseur de services sans le consentement de cette autorité; et
   ii. doivent informer rapidement l'autorité visée au paragraphe 4.c si le fournisseur de services a reçu pour instruction de ne pas divulguer les données demandées et doivent motiver cette décision.

e. Une Partie doit désigner une autorité unique pour recevoir la communication prévue au paragraphe 5.a et exécuter les tâches décrites aux paragraphes 5.b, 5.c. et 5.d. La Partie communique au Secrétaire Général du Conseil de l'Europe, au moment où la notification au Secrétaire Général prévue au paragraphe 5.a est faite pour la première fois, les coordonnées de cette autorité.

f. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties conformément au paragraphe 5.e et note si elles exigent la communication d'informations prévue au paragraphe 5.a et dans quelles circonstances. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

6. Si le fournisseur de services le juge acceptable, une partie peut soumettre une commande en vertu du paragraphe 1 et des informations supplémentaires en vertu du paragraphe 4 sous forme électronique. Une Partie peut fournir la notification et les informations supplémentaires en vertu du paragraphe 5 sous forme électronique. Des niveaux appropriés de sécurité et d'authentification peuvent être exigés.

7. Si un fournisseur de services informe l'autorité visée au paragraphe 4.c qu'il ne divulguera pas les données relatives aux abonnés demandées ou s'il ne divulgue pas les données relatives aux abonnés en réponse à une injonction adressée en application du paragraphe 1 dans les trente jours suivant sa réception ou dans le délai prévu au paragraphe 4.d, la plus longue période étant retenue, les autorités compétentes de la Partie émettrice peuvent ensuite demander l'exécution de leur injonction uniquement au

moyen de l'article 8 ou d'autres formes d'entraide. Les Parties peuvent demander au fournisseur de services de motiver son refus de divulguer les données relatives aux abonnés qui font l'objet de l'injonction.

8. Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'une Partie émettrice doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en vertu de l'article 8, à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait.

9. Au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut:

   a. se réserver le droit de ne pas appliquer cet article;
   b. si la divulgation de certains types de numéros d'accès en vertu de cet article était incompatible avec les principes fondamentaux de son ordre juridique interne, se réserver le droit de ne pas appliquer cet article à ces numéros.

Section 3 – Procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées

Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic

1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à délivrer une injonction à présenter à une autre Partie aux fins d'ordonner à un fournisseur de services sur le territoire de la Partie requise de communiquer

   a. des informations relatives à un abonné, et
   b. des données relatives au trafic

   spécifiées et stockées, en la possession ou sous le contrôle dudit fournisseur de service, lorsque ces informations et données sont nécessaires pour des enquêtes ou procédures pénales spécifiques menées par la Partie.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour donner effet à une injonction visée au paragraphe 1 soumise par une Partie requérante.

3. Dans sa demande, la Partie requérante soumet l'injonction visée au paragraphe 1, les informations qui l'accompagnent et toute instruction procédurale spéciale à la Partie requise.

   a. L'injonction spécifie:

      i. l'autorité émettrice et la date d'émission de la requête;
      ii. une déclaration selon laquelle l'injonction est soumise en vertu du présent Protocole;
      iii. le nom et l'adresse du ou des fournisseurs de services à laquelle elle doit être notifiée;
      iv. la ou les infractions visées par l'enquête ou des poursuites pénales;
      v. l'autorité à l'origine de la demande d'informations ou de données, si elle est différente de l'autorité ayant délivré l'injonction; et
      vi. de manière détaillée les informations ou les données spécifiques demandées.

b. Les informations fournies à l'appui de l'injonction pour aider la partie requise à lui donner effet et qui ne doivent pas être divulguées au fournisseur de services sans le consentement de la Partie requérante incluent:

i. les fondements juridiques en droit interne qui donnent à l'autorité le pouvoir d'émettre l'injonction;
ii. les dispositions légales et sanctions applicables pour la ou les infractions objet de l'enquête ou des poursuites;
iii. la raison pour laquelle la Partie requérante pense que le fournisseur de services est en possession des données ou les contrôle;
iv. une synthèse des faits liés à l'enquête ou aux poursuites;
v. la pertinence des informations ou données pour l'enquête ou les poursuites;
vi. les éléments permettant de contacter une ou des autorités pour de plus amples informations;
vii. si la conservation des informations ou des données a déjà été demandée, auquel cas le document précisera la date de la demande et la cote de référence; et
viii. si les informations ou les données ont déjà été demandées par d'autres moyens et si oui, lesquels.

c. La Partie requérante peut demander que la Partie requise suive des instructions procédurales spécifiques.

4. Une Partie peut déclarer au moment de la signature du Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, et à tout autre moment, que des informations supplémentaires sont nécessaires pour donner effet à des injonctions soumises en vertu du paragraphe 1.

5. La Partie requise accepte les demandes sous forme électronique; toutefois, avant de les accepter, elle peut exiger des niveaux de sécurité et d'authentification appropriés.

6. a. À compter de la date de réception de toutes les informations visées aux paragraphes 3 et 4, la Partie requise s'emploie raisonnablement à notifier l'injonction au fournisseur de service dans les quarante-cinq jours au plus en lui ordonnant de produire les informations en retour dans les:

i. vingt jours pour des informations relatives à l'abonné; et
ii. quarante-cinq jours pour les données relatives au trafic.

b. La Partie requise procède sans tarder à la transmission à la Partie requérante des informations ou données produites.

7. Si la Partie requise n'est pas en mesure d'appliquer sous la forme requise les instructions visées au paragraphe 3.c, elle en informe sans délai la Partie requérante et, au besoin, spécifie les conditions qui lui permettraient d'appliquer les instructions, à la suite de quoi la Partie requérante détermine si la demande doit malgré tout être exécutée.

8. La Partie requise peut invoquer les motifs visés à l'article 25, paragraphe 4, ou à l'article 27, paragraphe 4, de la Convention pour refuser l'exécution d'une demande ou peut imposer les conditions qu'elle estime nécessaires pour permettre l'exécution de la demande. La Partie requise peut invoquer les raisons visées à l'article 27, paragraphe 5, de la Convention pour ajourner l'exécution d'une demande. La Partie requise notifie dès que possible le refus, les conditions ou l'ajournement à la Partie requérante. La Partie requise notifie également à la Partie requérante les autres circonstances pouvant

retarder de manière significative l'exécution de la demande. L'article 28, paragraphe 2.b de la Convention s'applique au présent article.

9. a. Si la Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 8, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou le matériel devraient néanmoins être fournis.

b. Si la Partie requérante accepte la condition, elle est liée par celle-ci. La partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ce matériel.

10. Au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, chaque Partie communique au Secrétaire Général du Conseil de l'Europe et tient à jour les coordonnées des autorités désignées:

a. pour soumettre une injonction visée par le présent article; et
b. pour recevoir une injonction visée par le présent article.

11. Une Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige que les demandes visées par le présent article soient transmises par l'autorité ou les autorités centrales de la Partie requérante, ou par toute autre autorité désignée d'un commun accord entre les Parties concernées.

12. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées par les Parties en vertu du paragraphe 10. Chaque Partie veille à ce que les coordonnées portées au registre soient en permanence correctes.

13. Au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, une Partie peut se réserver le droit de ne pas appliquer le présent article aux données relatives au trafic.

Article 9 – Divulgation accélérée de données informatiques stockées en situation d'urgence

1. a. Chaque Partie adopte les mesures législatives et autres pouvant se révéler nécessaires, en cas d'urgence, pour que son point de contact du Réseau 24/7 visé à l'article 35 de la Convention (« point de contact ») puisse transmettre une demande à un Point de contact dans une autre Partie et recevoir une demande de ce dernier pour une assistance immédiate en vue de l'obtention par un fournisseur de services situé sur le territoire de la Partie concernée de la divulgation accélérée de données informatiques stockées spécifiées qui sont en la possession ou sous le contrôle dudit fournisseur de services, sans requête d'entraide judiciaire.

b. Une Partie peut, au moment de la signature de ce Protocole ou au moment du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle n'exécutera pas de demandes introduites en vertu du paragraphe 1.a) pour la divulgation d'informations relatives à l'abonné seulement.

2. Chaque Partie adopte les mesures législatives et autres pouvant se révéler nécessaires pour habiliter, conformément au paragraphe 1:

a. ses autorités à demander des données à un fournisseur de services situé sur son territoire à la suite d'une demande émise en vertu du paragraphe 1;

b. un fournisseur de services sur son territoire à divulguer les données demandées à ses autorités en réponse à une demande émise en vertu de l'alinéa 2.a; et

c. ses autorités à fournir les données demandées à la Partie requérante.

3. La demande introduite en vertu du paragraphe 1:

a. Spécifie l'autorité compétente qui cherche des données et la date à laquelle la demande a été faite;
b. contient une déclaration selon laquelle la demande est émise en vertu du présent Protocole;
c. précise le nom et l'adresse du/des fournisseur(s) de services en possession des données recherchées ou qui en ont le contrôle;
d. précise la ou les infractions faisant l'objet de l'enquête ou des procédures pénales et indique la référence à ses dispositions légales et les sanctions applicables;
e. mentionne suffisamment de faits démontrant que la situation est urgente et comment les données demandées sont liées à la situation;
f. s'accompagne d'une description détaillée des données demandées;
g. précise les éventuelles instructions procédurales; et
h. mentionne toute autre information pouvant aider à obtenir la divulgation des données demandées.

4. La Partie requise accepte des demandes sous forme électronique. Une Partie peut également accepter des demandes transmises oralement et peut exiger une confirmation sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

5. Une Partie peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer qu'elle exige des Parties requérantes que celles-ci, après l'exécution de la demande, lui soumettent la demande et toutes informations supplémentaires transmises à l'appui de cette dernière, dans le format et par le canal, qui peut couvrir une demande d'entraide judiciaire, spécifiés par la Partie requise.

6. La Partie requise informe la Partie requérante selon une procédure accélérée de sa détermination concernant la demande visée au paragraphe 1 et, au besoin, spécifie les éventuelles conditions dans lesquelles elle fournirait les données et toutes autres formes de coopération qui peuvent être utilisées.

7. a. Si une Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 6, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou les documents devraient néanmoins être fournis. Si la Partie requérante accepte la condition, elle est liée par celle-ci.

b. La partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la partie requérante qu'elle explique, en relation avec cette condition, l'utilisation qui a été faite de ces renseignements ou de ce matériel.

Section 4 – Procédures relatives à la demande d'entraide urgente

Article 10 – Demande d'entraide urgente

1. Chaque Partie peut demander une entraide judiciaire par les moyens les plus rapides lorsqu'elle estime qu'il y a urgence. Une demande d'entraide en vertu du présent article doit présenter, outre les autres contenus requise, une description des faits étayant l'existence d'une situation urgente et une explication de la manière dont l'entraide demandée est liée à cette situation.

2. La Partie requise accepte une telle demande d'entraide sous forme électronique. Elle peut exiger des niveaux de sécurité et d'authentification appropriés avant de l'accepter.

3. La Partie requise peut, par les moyens les plus rapides, demander un complément d'information afin d'évaluer la demande d'entraide. La Partie requérante fournit ce complément d'information par les moyens les plus rapides.

4. Après avoir conclu à l'existence d'une situation urgente et s'être assuré que les autres conditions de l'entraide sont satisfaites, la Partie requise répond à la demande d'entraide par les moyens les plus rapides.

5. Chaque Partie veille à ce qu'une personne de son autorité centrale ou d'autres autorités responsables des demandes d'entraide soit disponible vingt-quatre heures sur vingt-quatre, sept jours sur sept, pour répondre à une demande présentée en vertu du présent article.

6. Les autorités centrales ou autres autorités responsables des demandes d'entraide des Parties requérante et requise peuvent décider de prévoir que les résultats de l'exécution d'une demande d'entraide effectuée en vertu du présent article, ou une copie préliminaire de ces résultats, peuvent être transmis à la Partie requérante par un canal autre que celui utilisé pour la transmission la demande.

7. Lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, l'article 27, paragraphes 2.b et 3 à 8, et l'article 28, paragraphes 2 à 4, de la Convention s'appliquent au présent article.

8. Lorsqu'un tel traité ou arrangement existe, le présent article est complété par les dispositions de ce traité ou arrangement, à moins que les Parties concernées ne décident d'un commun accord d'appliquer à la place l'une ou la totalité des dispositions de la Convention visées au paragraphe 7 du présent article.

9. Chaque Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, déclarer que des demandes d'entraide peuvent aussi être adressées directement par ses autorités judiciaires, ou par le biais de l'Organisation internationale de police criminelle (INTERPOL) ou du point de contact 24/7 établi au titre de l'article 35 de la Convention. Dans de tels cas, une copie est envoyée en même temps à l'autorité centrale de la Partie requise par le truchement de l'autorité centrale de la Partie requérante. Lorsqu'une demande est adressée directement à une autorité judiciaire de la Partie requise et que celle-ci n'est pas compétente pour traiter la demande, elle transmet la demande à l'autorité nationale compétente et en informe directement la Partie requérante.

Section 5 – Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

Article 11 – Vidéoconférence

1. Une Partie requérante peut demander, et la Partie requise peut autoriser, le recueil de la déposition d'un témoin ou d'un expert par vidéoconférence. La Partie requérante et la Partie requise se concertent pour faciliter la résolution de tous problèmes pouvant se poser concernant l'exécution de la demande, y compris le cas échéant le choix de la Partie qui dirige l'opération; les autorités et personnes qui seront présentes; si l'une des Parties ou les deux doivent demander au témoin ou à l'expert de prêter un serment particulier, lui dispenser des avertissements ou des instructions; la manière de questionner le témoin ou l'expert; la manière dont les droits du témoin ou de l'expert seront dûment garantis; le traitement des revendications de privilèges ou d'immunité; le traitement des objections aux questions ou réponses; et la question de savoir si l'une des Parties ou les deux assurent des services de traduction, d'interprétation et de transcription.

2. a. Les autorités centrales de la Partie requise et de la Partie requérante communiquent directement entre elles aux fins du présent article. Une Partie requise peut accepter une demande sous forme électronique. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

   b. La Partie requise informe la Partie requérante des raisons pour lesquelles la demande n'a pas été exécutée ou a été retardée. L'article 27, paragraphe 8, de la Convention s'applique au présent article. Sans préjudice de toute autre condition qu'une Partie requise peut imposer conformément au présent article, les paragraphes 2 à 4 de l'article 28 de la Convention s'appliquent au présent article.

3. Une Partie requise fournissant son assistance au titre de cet article veille aux mesures nécessaires pour obtenir la présence de la personne dont le témoignage ou la déposition est requis. Le cas échéant, la Partie requise peut, dans la mesure où son droit le lui permet, prendre les mesures nécessaires pour obliger un témoin ou un expert à comparaître dans la Partie requise à l'endroit, à la date et à l'heure fixées.

4. Les procédures concernant la conduite de la vidéoconférence spécifiées par la Partie requérante sont appliquées, à moins qu'elles ne soient incompatibles avec le droit interne de la Partie requise. En cas d'incompatibilité, ou si la procédure n'a pas été spécifiée par la Partie requérante, la Partie requise applique la procédure prévue dans son droit interne sauf s'il en a été convenu autrement par les Parties requérante et requise.

5. Sans préjudice d'une éventuelle compétence en vertu du droit interne de la Partie requérante, lorsque, durant la vidéoconférence, le témoin ou l'expert:

   a. fait intentionnellement une fausse déclaration alors que la Partie requise a, conformément à son droit interne, intimé à la personne auditionnée de dire la vérité dans sa déposition;
   b. refuse de témoigner alors que la Partie requise a, conformément à son droit interne, astreint une telle personne à le faire; ou
   c. commet tout autre acte interdit par le droit interne de la Partie requise au cours de l'audition;

   Il encourt dans la Partie requise la même sanction que si l'acte avait été commis dans le cadre des procédures prévues par le droit interne de cette dernière.

6. a. À moins que la Partie requérante et la Partie requise en aient décidé autrement, la Partie requise supporte tous les coûts liés à l'exécution d'une demande d'entraide en vertu de cet article, sauf:

   i. les honoraires d'un témoin expert;
   ii. les coûts de traduction, d'interprétation et de transcription; et
   iii. les dépenses exceptionnelles.

   b. Si l'exécution d'une demande est susceptible d'entraîner des dépenses de nature exceptionnelle, la Partie requérante et la Partie requise se concertent pour déterminer dans quelles conditions la demande sera exécutée.

7. Lorsque la Partie requérante et la Partie requise en conviennent:

   a. les dispositions du présent article peuvent être appliquées dans le but de réaliser des audioconférences;

   b. la technologie de la vidéoconférence peut être utilisée à des fins, ou pour des auditions, différentes de celles visées au paragraphe 1, y compris en vue de l'identification de personnes ou d'objets.

8. Lorsqu'une Partie requise choisit d'autoriser l'audition d'un suspect ou d'un inculpé, elle peut poser des conditions et garanties particulières pour ce qui est du recueil du témoignage ou de la déposition de la personne, ou prévoir des notifications ou applications de mesures procédurales concernant cette personne.

Article 12 – Équipes communes d'enquête et enquêtes communes

1. Lorsqu'une coordination renforcée est considérée comme particulièrement utile, d'un commun accord, les autorités compétentes de deux ou plusieurs Parties peuvent établir et faire fonctionner une équipe commune d'enquête sur leurs territoires pour faciliter les enquêtes ou les poursuites. Les autorités compétentes sont déterminées par les Parties respectives concernées.

2. Les procédures et modalités régissant le fonctionnement d'équipes communes d'enquête, telles que leurs objectifs spécifiques; leur composition; leurs fonctions; leur durée et toute éventuelle prolongation; leur emplacement; leur organisation; le recueil, la transmission et l'utilisation des informations ou preuves; les conditions de confidentialité et les conditions de l'implication des autorités participantes d'une Partie dans des mesures d'enquête se déroulant sur le territoire d'une autre Partie, font l'objet d'un accord entre les autorités compétentes concernées.

3. Une Partie peut déclarer, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, que son autorité centrale doit être signataire de l'accord portant création de l'équipe ou y souscrire d'une autre manière.

4. Ces autorités compétentes et participantes communiquent directement entre elles, mais les Parties peuvent convenir d'un commun accord d'autres canaux de communication appropriés lorsque des circonstances exceptionnelles requièrent une coordination plus centrale.

5. Lorsque des actes d'enquête doivent être effectués sur le territoire de l'une des Parties concernées, les autorités participantes de cette Partie peuvent demander à leurs propres autorités d'effectuer ces actes sans que les autres Parties aient à soumettre une

demande d'entraide. Ces mesures doivent être mises en œuvre par les autorités de la cette Partie sur son territoire aux mêmes conditions que celles s'appliquant en droit interne à une enquête nationale.

6. L'utilisation d'informations ou de preuves fournies par les autorités participantes d'une Partie aux autorités participantes d'autres Parties concernées peut être refusée ou limitée dans les conditions prévues à l'accord décrit aux paragraphes 1 et 2. Si un tel accord ne prévoit pas de conditions pour le refus ou la limitation de cette utilisation, les Parties peuvent utiliser les informations ou preuves fournies:

   a. aux fins pour lesquelles l'accord a été conclu;

   b. pour détecter, enquêter et poursuivre des infractions pénales autres que celles pour lesquelles l'accord a été conclu, sous réserve du consentement préalable des autorités qui ont fourni ces informations ou preuves. Le consentement ne sera toutefois pas requis lorsque les principes juridiques fondamentaux de la Partie utilisant les informations ou preuves exigent qu'elle divulgue ces dernières pour protéger les droits d'une personne poursuivie dans le cadre d'une procédure pénale. Dans ce cas, les autorités concernées doivent le notifier sans retard indu aux autorités qui ont fourni les informations ou preuves; ou

   c. pour leur permettre de prévenir une urgence. Dans ce cas, les autorités participantes qui ont reçu les informations ou preuves doivent le notifier dans les plus brefs délais aux autorités participantes qui les ont fournies, sauf autre accord.

7. En l'absence d'accord tel que visé aux paragraphes 1 et 2, des enquêtes conjointes peuvent être mises en œuvre selon des modalités convenues au cas par cas. Ce paragraphe s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les Parties concernées.

Chapitre III – Conditions et garanties

Article 13 – Conditions et garanties

Conformément à l'article 15 de la Convention, chaque Partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus dans le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui doit assurer la protection adéquate des droits de l'homme et des libertés.

Article 14 – Protection des données à caractère personnel

1. Champ d'application

   a. Sauf disposition contraire des paragraphes 1.b et c, chaque partie traite les données à caractère personnel qu'elle reçoit au titre du présent Protocole conformément aux paragraphes 2 à 15 du présent article.

   b. Si, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie transférante et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application de cet accord, aux données à caractère personnel reçues en vertu du Protocole en lieu et place des paragraphes 2 à 15, sauf accord contraire entre les Parties concernées.

   c. Si la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord décrit au paragraphe 1.b, elles peuvent déterminer d'un commun accord que le transfert de données à caractère personnel en vertu du présent Protocole peut avoir lieu sur la base d'autres accords ou arrangements entre les Parties concernées en lieu et place des paragraphes 2 à 15.

   d. Chaque Partie considère que le traitement des données à caractère personnel conformément aux paragraphes 1.a et 1.b répond aux exigences de son cadre juridique de protection des données à caractère personnel pour les transferts internationaux de données à caractère personnel, et aucune autre autorisation de transfert n'est requise en vertu de ce cadre juridique. Une Partie ne peut refuser ou empêcher les transferts de données vers une autre Partie en vertu du présent Protocole que pour des raisons de protection des données: dans les conditions énoncées au paragraphe 15, lorsque le paragraphe 1.a s'applique; ou aux termes d'un accord ou d'un arrangement visé aux paragraphes 1.b ou c, lorsque l'un de ces paragraphes s'applique.

   e. Aucune disposition du présent article n'empêche une Partie d'appliquer des garanties plus strictes au traitement par ses propres autorités des données à caractère personnel reçues en vertu du présent Protocole.

2. But et utilisation

   a. La Partie destinataire de données à caractère personnel traite lesdites données aux fins prévues à l'article 2. Elle ne procède pas à d'autres traitements des

données à caractère personnel dans un but incompatible avec cet article, et elle ne traite pas non plus les données lorsque son cadre juridique ne l'autorise pas. Le présent article ne porte pas atteinte à la capacité de la Partie opérant le transfert d'imposer des conditions supplémentaires en vertu du présent Protocole dans une situation spécifique; toutefois, ces conditions n'incluent pas des conditions génériques de protection des données.

b. La Partie destinataire veille, dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement.

3. Qualité et intégrité

Chaque Partie prend des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte et complète et soient aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi, compte tenu des buts dans lesquels elles sont traitées.

4. Données sensibles

Le traitement par une Partie de données à caractère personnel révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale, ainsi que le traitement de données génétiques, de données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent; ou de données à caractère personnel concernant la santé ou la sexualité; ne peut avoir lieu que moyennant des garanties appropriées pour se prémunir contre le risque d'effets préjudiciables injustifiés résultant de l'utilisation de ces données, en particulier contre la discrimination illicite.

5. Durées de conservation

Chaque Partie conserve les données à caractère personnel uniquement pour la durée nécessaire et appropriée, aux fins du traitement des données prévu au paragraphe 2. Pour s'acquitter de cette obligation, la Partie prévoit dans le cadre de son droit interne des durées de conservation spécifiques ou une révision périodique de l'opportunité de continuer à conserver les données.

6. Décisions automatisées

Les décisions ayant un effet défavorable significatif sur les intérêts pertinents de l'individu concerné par les données à caractère personnel ne peuvent pas être fondées uniquement sur un traitement automatisé des données à caractère personnel, sauf autorisation dans le droit interne et avec des garanties appropriées qui prévoient la possibilité d'obtenir une intervention humaine.

7. Sécurité des données et incidents de sécurité

a. Chaque Partie s'assure de disposer de mesures technologiques, physiques et organisationnelles appropriées pour la protection des données à caractère personnel, en particulier contre la perte ou l'accès, la divulgation, l'altération ou la destruction accidentels ou non autorisés (« incident lié à la sécurité »).

b. Dès qu'il est pris connaissance d'un incident de sécurité entraînant un risque significatif de préjudice matériel ou non matériel à des personnes ou à l'autre Partie, la Partie qui a reçu les données en évalue sans tarder la probabilité de

survenance et l'importance, et prend rapidement les mesures appropriées pour atténuer ce préjudice. Ces mesures prennent la forme d'une notification à l'autorité transférante ou, aux fin du chapitre II, section 2, à l'autorité ou aux autorités désignées conformément au paragraphe 7.c; cependant, la notification peut prévoir des restrictions appropriées concernant la transmission ultérieure de la notification ; elle peut être différée ou omise lorsqu'elle risque de porter atteinte à la sécurité nationale, ou être retardée lorsque cette notification peut mettre en danger des opérations visant à protéger la sécurité publique. Ces mesures doivent également inclure une notification à la personne concernée, à moins que la Partie n'ait pris des mesures appropriées afin qu'il n'y ait plus de risque significatif. La notification à la personne concernée peut être différée ou omise dans les conditions énoncées au paragraphe 12.a.i. La Partie qui reçoit la notification peut demander une consultation et un complément d'information concernant l'incident et la réponse qui a été mise en œuvre.

c. Chaque Partie, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, indique au Secrétaire Général du Conseil de l'Europe quelles sont l'autorité ou les autorités qui reçoivent la notification visée au paragraphe 7.b, aux fins de la section 2 du chapitre II ; celles-ci peuvent être modifiées ultérieurement.

8. Tenue de registres

Chaque Partie tient des registres ou se dote d'autres moyens appropriés pour montrer comment il est accédé aux données à caractère personnel d'un individu et comment celles-ci sont utilisées et divulguées dans un cas spécifique.

9. Partage ultérieur au sein d'une Partie

a. Lorsqu'une autorité d'une Partie fournit des données à caractère personnel reçues initialement en vertu du présent Protocole à une autre autorité de cette Partie, cette dernière les traite conformément au présent article, sous réserve du paragraphe 9.b.

b. Nonobstant le paragraphe 9.a, une Partie qui a fait une réserve en vertu de l'article 17 peut fournir des données à caractère personnel qu'elle a reçues à ses États constitutifs ou à des entités territoriales similaires, à condition que la Partie ait mis en place des mesures pour que les autorités qui reçoivent les données continuent à les protéger efficacement en assurant un niveau de protection des données comparable à celui offert par le présent article.

c. En cas d'indications d'une application incorrecte du présent paragraphe, la Partie transférante peut demander une consultation et des informations pertinentes sur ces indications.

10. Transfert ultérieur vers un autre État ou vers une organisation internationale

a. La Partie recevant les données à caractère personnel ne peut les transférer à un autre État ou à une organisation internationale qu'avec l'autorisation préalable de l'autorité qui les lui a communiquées ou, aux fins de la section 2 du chapitre II, de l'autorité ou des autorités désignées en vertu du paragraphe 10.b.

b. Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, l'autorité ou les autorités aux pouvoirs d'autorisation

aux fins de la section 2 du chapitre II; ces informations peuvent être modifiées ultérieurement.

11. Transparence et notification

a. Chaque Partie assure les notifications par publication de notifications générales ou par notification spécifique à l'individu dont les données à caractère personnel ont été recueillies, concernant:

i. la base juridique et le(s) but(s) du traitement;
ii. toute durée de conservation ou de révision telle que visée au paragraphe 5, le cas échéant;
iii. les destinataires ou les catégories de destinataires auxquels ces informations sont divulguées; et
iv. l'accès, les rectifications ainsi que les recours possibles.

b. Une Partie peut soumettre toute exigence de notification personnelle à des restrictions raisonnables en vertu de son cadre juridique national conformément aux conditions énoncées au paragraphe 12.a.i.

c. Lorsque le droit interne de la Partie transférante exige que l'individu dont les données ont été fournies à une autre Partie soit informé personnellement, la Partie transférante prend des mesures pour que l'autre Partie soit informée au moment du transfert de cette exigence et des coordonnées appropriées. Toute demande de la part de la Partie destinataire des données pour que la Partie transférante ne procède pas à ladite notification s'applique uniquement dans les conditions énoncées au paragraphe 12.a.i. Dès que ces restrictions ne s'appliquent plus et que la communication des données à caractère personnel peut être effectuée, l'autre partie prend des mesures pour que la partie transférante soit informée. Si elle n'a pas encore été informée, la Partie transférante peut faire des demandes à la Partie destinataire qui informera la Partie transférante si la restriction doit être maintenue.

12. Accès et rectification

a. Chaque Partie veille à ce que toute personne dont les données à caractère personnel ont été reçues en application du présent Protocole ait le droit de demander et d'obtenir, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif:

i. l'accès à une copie écrite ou électronique de la documentation conservée sur cette personne, contenant ses données à caractère personnel et les informations disponibles indiquant la base juridique et les finalités du traitement, la conservation et les destinataires ou catégories de destinataires des données (« accès »), ainsi que les informations concernant les possibilités de recours disponibles à condition que l'accès dans un cas particulier puisse être soumis à l'application de restrictions proportionnées autorisées par son cadre juridique interne, nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée;

ii. la rectification lorsque les données à caractère personnel de la personne sont inexactes ou ont été traitées de manière inappropriée; la rectification doit inclure, selon ce qui est approprié et raisonnable compte tenu des

motifs de la demande de rectification et du contexte particulier du traitement, la correction, le complément, l'effacement ou l'anonymisation, la restriction du traitement ou le blocage.

b. Si l'accès ou la rectification est refusé ou restreint, la Partie en informe la personne concernée sous une forme écrite qui peut être envoyée par voie électronique, sans retard excessif, en informant l'individu du refus ou de la restriction. Elle indique les motifs de ce refus ou de cette restriction et fournit des informations sur les voies de recours disponibles. Les frais d'accès doivent être limités à ce qui est raisonnable et non excessif.

13. Recours judiciaire et non-judiciaire

Chaque partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article.

14. Supervision

Chaque Partie dispose d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et effectives à l'égard des mesures établies dans le présent article. Les fonctions et compétences exercées ensemble ou séparément par ces autorités comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives.

15. Consultation et suspension

Une Partie peut suspendre le transfert de données à caractère personnel à une autre Partie si elle dispose de preuves substantielles que celle-ci viole de manière systématique ou flagrante les dispositions du présent article ou qu'une violation flagrante est imminente. Cette suspension n'interviendra qu'à l'expiration d'un préavis raisonnable sans parvenir à une solution. Toutefois, une Partie peut suspendre provisoirement les transferts en cas de violation systématique ou flagrante présentant un risque important et imminent pour la vie ou la sécurité d'une personne physique, ou de préjudice financier ou de réputation pour cette personne, auquel cas cette Partie en informe l'autre et entame des consultations avec celle-ci immédiatement après. Si les délais de consultation ne permettent pas de trouver une solution, l'autre Partie peut suspendre les transferts si elle dispose de preuves substantielles que la suspension par la première Partie qui a procédé à la suspension était contraire aux termes du présent paragraphe. La Partie qui a procédé à la suspension la lève dès qu'il a été remédié à la violation justifiant la suspension ; toute suspension réciproque est levée à ce moment. Toutes les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au présent Protocole.

Chapitre IV – Dispositions finales

Article 15 – Effets de ce Protocole

1. a. L'article 39, paragraphe 2, de la Convention s'applique au présent Protocole.

   b. En ce qui concerne les Parties qui sont membres de l'Union européenne: ces Parties peuvent, dans leurs relations mutuelles, appliquer les lois de l'Union européenne régissant les questions traitées dans le présent protocole.

   c. Le paragraphe 1.b n'affecte pas la pleine application du présent Protocole entre les Parties qui sont membres de l'Union européenne et les autres Parties.

2. L'article 39, paragraphe 3, de la Convention s'applique au présent Protocole.

Article 16 – Signature et entrée en vigueur

1. Le présent Protocole est ouvert à la signature des Parties à la Convention, qui peuvent exprimer leur consentement à être 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. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3. Le présent Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Parties à la Convention auront exprimé leur consentement à être liées par ce Protocole conformément aux dispositions des paragraphes 1 et 2 du présent article.

4. Pour toute Partie à la Convention 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 à laquelle la Partie a exprimé son consentement à être liée par le Protocole, conformément aux dispositions des paragraphes 1 et 2 de cet article.

Article 17 – Clause fédérale

1. Un État fédéral peut se réserver le droit d'assumer les obligations découlant du présent Protocole conformément à ses principes fondamentaux régissant les relations entre son gouvernement central et les États constitutifs ou autres entités territoriales similaires, à condition que:

   a. le Protocole s'applique au gouvernement central de l'État fédéral;
   b. une telle réserve n'affecte pas les obligations de fournir la coopération demandée par les autres Parties conformément aux dispositions du chapitre II; et
   c. les dispositions de l'article 13 s'appliquent aux États constitutifs de l'État fédéral ou aux autres entités territoriales similaires.

2. Une autre Partie peut empêcher les autorités, les fournisseurs ou les entités sur son territoire de transférer des données à caractère personnel en réponse à une demande ou une injonction présentée directement par un État constitutif ou une autre entité territoriale similaire d'un État fédéral qui a formulé une réserve en vertu du paragraphe

1, à moins que l'État fédéral ne notifie au Secrétaire Général du Conseil de l'Europe que l'État constitutif ou l'autre entité territoriale similaire applique les obligations du présent Protocole applicables à cet État fédéral. Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre de ces notifications.

3. Une autre Partie n'empêche pas les autorités, les fournisseurs ou les entités sur son territoire de coopérer avec un État constitutif ou une autre entité territoriale similaire en raison d'une réserve formulée en vertu du paragraphe 1, si un ordre ou une demande a été soumis par l'intermédiaire du gouvernement central ou si un accord relatif à une équipe commune d'enquête en vertu de l'article 12 est conclu avec la participation du gouvernement central. Dans ces situations, le gouvernement central assure l'exécution des obligations applicables du Protocole, étant entendu qu'en ce qui concerne la protection des données à caractère personnel fournies aux États constitutifs ou aux entités territoriales similaires, seuls les termes de l'article 14, paragraphe 9, ou, le cas échéant, les termes d'un accord ou d'un arrangement décrit à l'article 14, paragraphe 1.b ou 1.c, s'appliquent.

4. En ce qui concerne les dispositions du présent Protocole dont l'application relève de la compétence des États constitutifs ou d'autres entités territoriales similaires, qui ne sont pas tenus par le système constitutionnel de la fédération de prendre des mesures législatives, le gouvernement central informe les autorités compétentes de ces États desdites dispositions avec son avis favorable, en les encourageant à prendre les mesures appropriées pour leur donner effet.

Article 18 – Application territoriale

1. Ce Protocole s'applique au(x) territoire(s) spécifiés dans une déclaration faite par une Partie en vertu de l'article 38, paragraphes 1 ou 2, de la Convention pour autant que cette déclaration n'ait pas été retirée en vertu de l'article 38, paragraphe 3.

2. Une Partie peut, au moment de la signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, spécifier que ce Protocole ne s'applique pas à un ou plusieurs territoires spécifiés dans la déclaration de la Partie en vertu de l'article 38, paragraphes 1 et 2 de la Convention.

3. Une déclaration en vertu du paragraphe 2 de cet article peut, concernant tout territoire qui y est spécifié, être retirée par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait deviendra effectif le premier jour du mois suivant l'expiration d'une période de trois mois après la date de la réception de cette notification par le Secrétaire Général.

Article 19 – Réserves et déclarations

1. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, ou d'approbation, déclarer qu'elle se prévaut de la ou des réserves prévues à l'article 7, paragraphes 9.a et 9.b, à l'article 8, paragraphe 13 et à l'article 17 du présent Protocole. Aucune autre réserve ne peut être formulée.

2. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention peut, au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation, faire la ou les déclarations prévues à l'article 7, paragraphes 2.b et 8, à l'article 8, paragraphe 11, à l'article 9, paragraphes 1.b et 5, à l'article 10, paragraphe 9.b, à l'article 12, paragraphe 3, et à l'article 18, paragraphe 2 du présent Protocole.

3. Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, toute Partie à la Convention fait la ou les déclarations, notifications ou communications visées à l'article 7, paragraphes 5.a et 5.e, à l'article 8, paragraphes 4 et 10.a and b, à l'article 14, paragraphes 7.c et 10.b, et à l'article 17, paragraphe 2, du présent Protocole selon les modalités qui y sont spécifiées.

Article 20 – Statut et retrait des réserves

1. Une Partie qui a fait une réserve conformément à l'article 19, paragraphe 1, retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent. Ce retrait prend effet à la date de réception d'une notification par le Secrétaire Général du Conseil de l'Europe. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2. Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves en application de l'article 19, paragraphe 1, des informations sur les perspectives de leur retrait.

Article 21 – Amendements

1. Toute Partie au Protocole peut proposer des amendements, qui sont communiqués au Secrétaire Général du Conseil de l'Europe, aux États membres du Conseil de l'Europe et aux États parties et signataires de la Convention ainsi qu'à tout État ayant été invité à adhérer à la Convention.

2. Tout amendement proposé par une Partie est communiqué au Comité européen sur les problèmes criminels (CDPC) qui soumet au Comité des Ministres son avis sur cet amendement proposé.

3. Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Parties à la Convention, peut adopter l'amendement.

4. Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 est transmis aux Parties à ce Protocole pour acceptation.

5. Tout amendement adopté conformément au paragraphe 3 entre en vigueur le trentième jour après que toutes les Parties à ce Protocole ont informé le Secrétaire Général qu'elles acceptent l'amendement.

Article 22 – Règlement des différends

L'article 45 de la Convention s'applique au présent Protocole.

Article 23 – Consultations des Parties et évaluation de la mise en œuvre

1. L'article 46 de la Convention s'applique au présent Protocole.

2. Les Parties évaluent périodiquement l'utilisation et la mise en œuvre effectives des dispositions du présent Protocole. L'article 2 du Règlement intérieur du Comité de la Convention sur la cybercriminalité tel que révisé le 16 octobre 2020 s'applique *mutatis mutandis.* Les Parties réexaminent initialement et peuvent modifier les procédures de cet article telles qu'elles s'appliquent au présent Protocole par consensus cinq ans après l'entrée en vigueur du présent Protocole.

3. L’examen de l’article 14 débute lorsque dix Parties à la Convention ont exprimé leur consentement à être liées par le présent Protocole.

Article 24 – Dénonciation

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

2. Ladite dénonciation prendra effet le premier jour du mois suivant l’expiration d’une période de trois mois après la date de réception de la notification par le Secrétaire Général.

3. La dénonciation de la Convention par une Partie au présent Protocole constitue une dénonciation du présent Protocole.

4. Les informations ou éléments de preuve transférés avant la date de prise d'effet de la dénonciation continuent d'être traités conformément au présent Protocole.

Article 25 – Notification

Le Secrétaire Général du Conseil de l’Europe notifie aux États membres du Conseil de l’Europe, aux Parties à la Convention et Signataires de la Convention, et à tout État qui a été invité à adhérer à la Convention:

a. toute signature;
b. le dépôt de tout instrument de ratification, d’acceptation ou d’approbation;
c. la date d’entrée en vigueur du présent Protocole conformément à l’article 16, paragraphes 3 et 4;
d. toutes déclarations ou réserves formulées conformément à l’article 19 ou retrait de réserves formulé conformément à l’article 20;
e. tout autre acte, notification ou communication concernant le présent Protocole.

En foi de quoi, les soussignés, dûment autorisés, ont apposé leur signature au bas du présent Protocole.

Fait à xx, le xx 20xx, 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 communiquera une copie certifiée conforme à chacun des États membres du Conseil de l'Europe, aux Parties et Signataires de la Convention, ainsi qu'à tout État invité à adhérer à la Convention.

Rapport explicatif

1. Le deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif à une coopération et la divulgation de preuves électroniques renforcée (« le présent Protocole ») a été adopté par le Comité des Ministres du Conseil de l'Europe lors de sa [xxx] réunion ([jour mois année]) des Délégués des Ministres et le Protocole a été ouvert à la signature à [lieu] le [jour mois année] [sur la question de la [conférence] et [ ]]. Le Comité des Ministres a également pris note du rapport explicatif.

2. Le texte du présent rapport explicatif est destiné à guider et à aider les Parties dans l'application du présent Protocole et reflète la compréhension des rédacteurs quant à son fonctionnement.

Introduction

Contexte

3. Depuis son ouverture à la signature à Budapest, le 23 novembre 2001, la Convention sur la cybercriminalité (STE n° 185; ci-après « la Convention »), est devenue un instrument auquel ont adhéré des pays de toutes les régions du monde et qui a des incidences sur chacune d'elles.

4. En 2003, la Convention a été complétée par le Protocole additionnel à la Convention sur la cybercriminalité relatif à l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (STE n° 189; dénommé ci-après le « Premier Protocole »).

5. Les technologies de l'information et des communications ont extraordinairement évolué et transformé la société partout dans le monde depuis l'ouverture de la Convention à la signature en 2001. Toutefois, depuis lors, on a également constaté une augmentation significative de l'exploitation de technologies à des fins criminelles. La cybercriminalité est désormais considérée par de nombreuses Parties comme une grave menace pour les droits fondamentaux des personnes, l'État de droit et le fonctionnement des sociétés démocratiques. Les menaces posées par la cybercriminalité sont nombreuses. On peut citer comme exemple la violence sexuelle exercée en ligne contre des enfants et les autres atteintes à la dignité et à l'intégrité des personnes; le vol et l'utilisation détournée de données personnelles qui constituent une ingérence dans le droit au respect de la vie privée; l'ingérence dans les processus électoraux et autres attaques contre les institutions démocratiques; les attaques contre les infrastructures critiques telles que celles par déni de service distribué et par des logiciels rançonneurs; ou l'utilisation abusive de ces technologies à des fins terroristes. En 2020-2021, pendant la pandémie du COVID-19, les pays ont observé une flambée massive de cybercriminalité liée au COVID-19, qui a pris des formes variées: attaques contre les hôpitaux et établissements médicaux qui développent des vaccins contre le virus, utilisation abusive de noms de domaine pour promouvoir de faux vaccins, traitements et remèdes, ainsi que d'autres types d'activités frauduleuses.

6. Malgré la croissance des technologies fondées sur les données et l'expansion et l'évolution pernicieuses de la cybercriminalité, les concepts énoncés dans la Convention sont neutres sur le plan technologique, de sorte que les infractions de droit pénal matériel peuvent être appliquées aux technologies concernées tant actuelles que futures, et la Convention reste essentielle dans la lutte contre la cybercriminalité. La Convention vise principalement à (1) harmoniser les éléments de droit pénal matériel interne des infractions et les dispositions connexes dans le domaine de la cybercriminalité, (2) prévoir les procédures pénales internes nécessaires pour les enquêtes et les poursuites concernant ces infractions ainsi que d'autres infractions commises au moyen d'un système informatique ou relatives à l'utilisation de preuves électroniques d'autres infractions et (3) mettre en place des mécanismes de coopération internationale.

7. En appliquant la Convention, les Parties respectent la responsabilité qu'ont les gouvernements de protéger les individus contre la criminalité, qu'elle soit commise en ligne ou hors ligne, par des enquêtes et des poursuites pénales efficaces. En effet, certaines Parties à la Convention considèrent qu'elles sont liées par une obligation internationale de fournir les moyens de protection contre les infractions commises au moyen d'un système informatique (voir K.U. c. Finlande, Cour européenne des droits de l'homme (requête n° 2872/02) (qui fait référence aux procédures et pouvoirs en matière d'enquêtes ou de procédures pénales que les Parties doivent établir en vertu de la Convention)).

8. Les Parties ont constamment cherché à remplir leur engagement de lutter contre la cybercriminalité en s'appuyant sur divers mécanismes et organes créés en vertu de la Convention et en prenant les mesures nécessaires pour permettre des enquêtes et des procédures pénales plus efficaces. Il est important de noter que l'utilisation et la mise en œuvre de la Convention sont facilitées par le Comité de la Convention sur la cybercriminalité (T-CY) établi en vertu de l'article 46 de cette Convention. En outre, la Convention est soutenue par des programmes de renforcement des capacités mis en œuvre par le Bureau du programme sur la cybercriminalité du Conseil de l'Europe à Bucarest, en Roumanie, qui aident les pays du monde entier à mettre en œuvre la Convention. Ce triangle composé (a) des normes communes de la Convention dans le domaine de la cybercriminalité, associé (b) à un mécanisme solide d'engagement permanent des Parties par le biais de la T-CY, et (c) à l'accent mis sur les programmes de renforcement des capacités, a contribué de manière significative à la portée et à l'impact de la Convention.

9. En 2012, le T-CY, agissant conformément au mandat que lui confère l'article 46, paragraphe 1, de la Convention concernant « l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique » et « l'examen de l'éventualité de compléter ou d'amender la Convention », a créé le Groupe ad hoc sur l'accès frontalier aux données et sur les questions de compétence territoriale (« Groupe sur l'accès transfrontalier »). En décembre 2014, le T-CY avait déjà terminé une évaluation des dispositions d'entraide de la Convention sur la cybercriminalité et adopté une série de recommandations, dont certaines devaient être traitées dans un nouveau protocole à la Convention. Ces efforts ont mené à la création, en 2015, du Groupe de travail sur l'accès de la justice pénale aux preuves stockées dans les « nuages », y compris par le biais de l'entraide judiciaire (« Groupe sur les preuves dans le nuage »).

10. En 2016, le Groupe sur les preuves dans le nuage a conclu, entre autres points, que « la cybercriminalité, le nombre de terminaux, de services et d'utilisateurs (notamment de terminaux et services mobiles) et, partant, le nombre de victimes ont atteint des proportions telles que seule une infime partie de la cybercriminalité ou autres infractions impliquant des preuves électroniques sera jamais enregistrée et donnera jamais lieu à des enquêtes. L'immense majorité des victimes ne peut pas s'attendre à ce que justice soit rendue. Les principales difficultés mises en évidence par le groupe concernaient « l'informatique en nuage, la territorialité et la compétence » et, de ce fait, l'obtention d'un accès efficace aux preuves électroniques et leur divulgation.

11. En examinant les conclusions du Groupe sur les preuves dans le nuage, les Parties à la Convention ont conclu qu'il n'était pas nécessaire de modifier la Convention ni de prévoir de nouvelles incriminations par le biais du droit pénal matériel. Toutefois, les Parties sont convenues que des mesures supplémentaires devaient être prises pour renforcer la coopération et la capacité des autorités de justice pénale à obtenir des preuves électroniques en élaborant un deuxième Protocole additionnel, ce afin de rendre plus efficace l'action de la justice pénale et de préserver l'État de droit.

Les travaux préparatoires

12. Lors de sa 17e réunion plénière (8 juin 2017), le T-CY a approuvé le mandat pour la préparation du présent Protocole sur la base d'une proposition formulée par le Groupe sur les preuves dans le nuage. Il a décidé d'engager de sa propre initiative le processus de rédaction de ce Protocole en se prévalant de l'article 46, paragraphe 1.c, de la Convention. Le 14 juin 2017, la Secrétaire générale adjointe du Conseil de l'Europe a informé le Comité des Ministres (1289ème réunion des Délégués des Ministres) de cette initiative du T-CY.

13. Couvrant initialement la période allant de septembre 2017 à décembre 2019, le mandat a été ultérieurement prorogé par le T-CY jusqu'en décembre 2020, puis à nouveau jusqu'en mai 2021.

14. En application des dispositions de ce mandat, le T-CY a créé une Plénière de rédaction du Protocole (PDP) composée de représentants des Parties à la Convention, et d'États, d'organisations et d'organes du Conseil de l'Europe dotés du statut d'observateur auprès du T-CY en qualité d'observateurs. La PDP était assistée dans la préparation du projet de protocole par un Groupe de rédaction du Protocole (PDG), composé d'experts des Parties à la Convention. Le PDG a créé à son tour plusieurs sous-groupes et groupes ad hoc chargé d'élaborer des dispositions spécifiques.

15. Entre septembre 2017 et mai 2021, le T-CY a tenu 10 Plénières de rédaction, 16 réunions du Groupe de rédaction et un grand nombre de réunions de sous-groupe et de groupe ad hoc. La plus grande partie du présent Protocole a été préparée pendant la pandémie de COVID-19. Du fait des restrictions liées à la COVID-19, entre mars 2020 et mai 2021, plus de 65 réunions ont eu lieu par visioconférence.

16. Les méthodes de travail susvisées (plénières, groupes de rédaction et sous-groupes et groupes ad hoc) ont permis aux représentants et aux experts des Parties d'apporter des contributions très importantes à la rédaction du Protocole et de mettre au point des solutions innovantes.

17. La Commission de l'Union européenne a participé à ces travaux au nom des États parties à la Convention qui étaient membres de l'Union européenne en vertu d'un mandat de négociation conféré par le Conseil de l'Union européenne le 6 juin 2019.

18. Une fois le projet de dispositions établi et adopté à titre provisoire par le PDP, ce projet d'articles a été publié et les parties prenantes ont été invitées à formuler des observations à son sujet.

19. Le T-CY a organisé six séries de consultations avec les parties prenantes de la société civile, du secteur privé ainsi que des experts en protection des données: en marge de la Conférence Octopus sur la cybercriminalité à Strasbourg en juillet 2018, avec des experts en protection des données à Strasbourg en novembre 2018, sous la forme d'une invitation à présenter des observations écrites sur le projet d'articles en février 2019, en marge de la Conférence Octopus sur la cybercriminalité à Strasbourg en novembre 2019, sous la forme d'une invitation à présenter des observations écrites sur le nouveau projet d'articles en décembre 2020, et en mai 2021 via des soumissions écrites et une réunion virtuelle tenue le 6 mai 2021.

20. Par ailleurs, le T-CY a consulté le Comité européen pour les problèmes criminels (CDPC) et le Comité consultatif de la Convention pour la protection des personnes à 'égard du traitement automatisé des données à caractère personnel (T-PD) du Conseil de l'Europe.

21. La 24ème plénière du T-CY tenue le 28 mai 2021 a approuvé le projet du présent Protocole et décidé de le soumettre au Comité des Ministres pour adoption.

Questions de fond

22. Du point de vue du fond, les travaux d'élaboration du présent Protocole sont partis, d'une part, des résultats de l'évaluation par le T-CY, en 2014, des dispositions de la Convention relatives à l'entraide, ainsi que des analyses et recommandations du Groupe sur l'accès transfrontalier et du Groupe sur les preuves dans le nuage, en 2014 et 2017, respectivement. En particulier, les défis en matière de territorialité et de compétence se rapportant aux preuves électroniques, c'est-à-dire le fait que les données nécessaires aux fins d'une enquête pénale peuvent être stockées dans des juridictions multiples, changeantes ou inconnues (« dans le nuage »), et le fait que des solutions doivent être apportées pour obtenir la divulgation de ces données de façon efficace et efficiente aux fins d'enquêtes ou de procédures pénales données, ont été jugés préoccupants.

23. Devant la complexité de ces défis, les rédacteurs du présent Protocole sont convenus d'axer leur attention sur les questions spécifiques énumérées ci-après:

– Au moment de la rédaction du Protocole, les demandes d'entraide judiciaire étaient la principale méthode pour obtenir des preuves électroniques d'une infraction pénale auprès d'autres États, y compris les outils d'entraide judiciaire de la convention. Toutefois, l'entraide judiciaire n'est pas toujours un bon moyen de traiter un nombre croissant de demandes de preuves électroniques volatiles. On a donc jugé nécessaire de mettre au point un mécanisme plus rationnel pour émettre des ordres ou des demandes aux fournisseurs de services d'autres parties afin de produire des informations sur les abonnés et des données relatives au trafic.

– Les données relatives aux abonnés – servant par exemple à identifier l'utilisateur d'un compte de messagerie électronique ou de média social, ou d'une adresse de protocole Internet (IP) utilisée pour commettre une infraction – sont les données le plus souvent recherchées dans les enquêtes pénales nationales et internationales liées à la cybercriminalité et à d'autres crimes impliquant des preuves électroniques. En l'absence de ces données, il est souvent impossible de poursuivre une enquête. Dans la plupart des cas, le recours à l'entraide judiciaire pour obtenir les données relatives aux abonnés n'est pas efficace et engorge le système d'entraide judiciaire. Ces données sont d'ordinaire détenues par les fournisseurs de services. L'article 18 de la Convention traite bien certains aspects de l'obtention des données relatives aux abonnés auprès des fournisseurs de services (voir la note d'orientation du T-CY relative à l'article 18), y compris dans les autres Parties, mais il a été jugé nécessaire de concevoir des outils complémentaires pour obtenir la divulgation de données relatives aux abonnés directement auprès d'un fournisseur de services d'une autre Partie. Ces outils permettraient d'accroître l'efficacité du processus et aussi d'alléger la pression sur le système d'entraide.

– Les données relatives au trafic sont également souvent recherchées dans le cadre d'enquêtes criminelles, et leur divulgation rapide peut s'avérer nécessaire pour remonter à la source d'une communication et servir de point de départ à la collecte de preuves supplémentaires ou à l'identification d'un suspect.

– De même, comme de nombreuses formes de criminalité en ligne sont facilitées par des domaines créés ou exploités à des fins criminelles, il est nécessaire d'identifier la personne qui a enregistré un domaine de ce type. De telles informations sont détenues par des entités fournissant des services d'enregistrement de noms de domaine, c'est-à-dire, en général, des bureaux d'enregistrement. Il s'impose donc de mettre en place un dispositif efficace permettant d'obtenir ces informations auprès des entités en question dans les autres Parties.

– Lorsque, dans une situation d'urgence, il existe un risque grave et imminent pour la vie ou la sécurité d'une personne physique, il faut intervenir rapidement soit en fournissant une entraide d'urgence, soit en utilisant le réseau de points de contact disponibles 24 heures sur 24 créé en application de la Convention.

– En outre, les outils éprouvés d'entraide mutuelle et de coopération internationale devraient être utilisés plus largement et entre toutes les parties. D'importantes mesures telles que la visioconférence ou les équipes communes d'enquête sont d'ores et déjà disponibles en vertu d'instruments du Conseil de l'Europe (par exemple, le deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, STE n°182) ou d'autres accords bilatéraux et multilatéraux. Cependant, de tels mécanismes ne sont pas universellement disponibles parmi les Parties à la Convention, et le Protocole vise à combler cette lacune.

– La Convention prévoit la collecte et l'échange d'informations et de preuves pour des enquêtes ou des procédures pénales spécifiques. Les rédacteurs ont reconnu que l'établissement, la mise en œuvre et l'application des pouvoirs et des procédures liés aux enquêtes et aux poursuites pénales doivent toujours être soumis à des conditions et à des garanties qui assurent une protection adéquate des droits de l'homme et des libertés fondamentales. Il était donc nécessaire d'inclure un article sur les conditions et les garanties, (similaire à l'article 15 de la Convention). En outre, reconnaissant l'exigence de nombreuses Parties de protéger la vie privée et les données à caractère personnel afin de satisfaire à leurs obligations constitutionnelles et internationales, les rédacteurs ont décidé de prévoir des garanties spécifiques de protection des données dans ce Protocole. Ces garanties de protection des données complètent les obligations de nombreuses Parties à la Convention, qui sont également parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108). Le protocole d'amendement à cette Convention (STCE n° 223) a été ouvert à la signature lors de la rédaction de ce Protocole en octobre 2018. Il convient également de noter que le processus de rédaction de ce Protocole a associé des Parties non soumises, à l'époque, aux instruments du Conseil de l'Europe relatifs à la protection des données ni aux règles de protection des données de l'Union européenne. En conséquence, des efforts importants ont été consentis pour élaborer un Protocole équilibré qui tienne compte des nombreux systèmes juridiques des États appelés à devenir Parties au Protocole tout en notant qu'il importait d'assurer la protection des droits au respect de la vie privée et à la protection des données comme l'exigent les constitutions et les obligations internationales des autres Parties à la Convention.

24. Les rédacteurs ont également examiné d'autres mesures qui, à l'issue d'une discussion approfondie, n'ont pas été retenues dans le présent Protocole. Deux de ces dispositions, à savoir « enquêtes clandestines à l'aide d'un système informatique » et « extension du champ des perquisitions», présentaient un grand intérêt pour les Parties, mais auraient exigé des efforts et du temps supplémentaires et de nouvelles consultations avec les parties prenantes. Il n'a donc pas été jugé possible de les traiter dans le délai imparti pour la préparation du présent Protocole. Les rédacteurs ont proposé d'en poursuivre l'examen sous une autre forme et, éventuellement, dans le cadre d'un instrument juridique distinct.

25. Dans l'ensemble, les rédacteurs ont considéré que les dispositions du présent Protocole apporteraient une forte valeur ajoutée sur le plan opérationnel aussi bien que sur celui des principes directeurs. Le Protocole améliorera considérablement la capacité des Parties à renforcer la coopération entre elles et entre les parties et les fournisseurs de services et autres entités et à obtenir la divulgation de preuves électroniques aux fins d'enquêtes ou de procédures pénales spécifiques. Ainsi, ce Protocole, comme la Convention, vise à accroître la capacité des autorités de justice pénale à lutter contre la cybercriminalité et d'autres infractions, tout en respectant pleinement les droits de l'homme et les libertés fondamentales, et il souligne l'importance et la valeur d'un Internet fondé sur la libre circulation des informations.

Le Protocole

26. Comme énoncé dans le préambule, le présent Protocole vise à renforcer davantage la coopération en matière de cybercriminalité et de collecte de preuves sous forme électronique et la capacité des autorités de justice pénale à recueillir des preuves sous forme électronique d'une infraction pénale aux fins d'enquêtes ou de procédures pénales spécifiques au moyen d'outils supplémentaires ayant trait à une entraide judiciaire plus efficace et à d'autres formes de coopération entre autorités compétentes; la coopération dans les situations d'urgence (c'est-à-dire les situations où existe un risque important et imminent pour la vie ou la sécurité d'une personne physique) et la coopération directe entre les autorités compétentes et les fournisseurs de services et d'autres entités ayant en leur possession ou sous leur contrôle des informations pertinentes. Le présent Protocole a donc pour but de compléter la Convention et, entre les Parties à celle-ci, le premier Protocole.

27. Le présent Protocole est divisé en quatre chapitres: I. Dispositions communes; II. Mesures de coopération renforcée; III. Conditions et garanties, et IV. Dispositions finales.

28. Les dispositions communes du chapitre I portent sur le but et la portée de ce Protocole. Comme c'est le cas de la Convention, le Protocole a trait à des enquêtes ou procédures pénales spécifiques, concernant non seulement la cybercriminalité, mais toute infraction pénale pour laquelle les preuves se présentent sous forme électronique, également appelée communément « preuve électronique » ou « preuve numérique ». Ce chapitre rend les définitions de la Convention applicables au présent Protocole et donne des définitions supplémentaires pour les termes qui reviennent fréquemment dans le Protocole. De plus, étant donné que les exigences en matière de connaissance de la langue au titre de l'entraide judiciaire et d'autres formes de coopération entravent souvent l'efficacité des procédures, un article sur la « langue » a été ajouté pour permettre d'adopter une approche plus pragmatique à cet égard.

29. Le chapitre II comprend les principaux articles de fond du Protocole, qui décrivent plusieurs types de coopération auxquels s'appliquent différents principes. Aussi a-t-il été nécessaire de diviser ce chapitre en sections, intitulées respectivement 1) principes généraux applicables au chapitre II, 2) procédures de renforcement de la coopération directe avec les fournisseurs de services et les entités fournissant des services d'enregistrement de noms de domaine dans d'autres Parties, 3) procédures de renforcement de la coopération internationale entre les autorités pour obtenir la divulgation de données informatiques stockées, 4) procédures relatives à l'entraide judiciaire d'urgence, et 5) procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables.

30. Le chapitre III prévoit des conditions et des garanties. Elles exigent des Parties qu'elles appliquent également des conditions et garanties analogues à celles qui font l'objet de l'article 15 de la Convention aux pouvoirs et procédures énoncés dans le présent Protocole. En outre, le présent chapitre inclut un ensemble détaillé de garanties applicables à la protection des données à caractère personnel.

31. La plupart des dispositions finales du chapitre IV sont peu différentes des dispositions finales classiques des instruments du Conseil de l'Europe ou rendent les dispositions de la Convention applicables au présent Protocole. Font exception l'Article 15 intitulé « Effets de ce Protocole », l'Article 17 « Clause fédérale » et l'Article 23 « Concertation des Parties et évaluation de l'application », qui diffèrent à des degrés divers des dispositions analogues de la Convention. Non seulement ce dernier article rend-t-il l'article 46 de la Convention applicable, mais ils dispose également que l'application et l'utilisation effective des dispositions du présent Protocole est évaluée périodiquement par les Parties.

Commentaire sur les articles du Protocole

Chapitre I – Dispositions communes

Article 1 – But

32. Le présent Protocole a pour objet de compléter a) la Convention entre les Parties au présent Protocole et, b) le Premier Protocole entre les Parties à celui-ci qui sont également Partie au présent Protocole.

Article 2 – Champ d'application

33. La portée générale d'application de ce Protocole est la même que celle de la Convention: les mesures prévues par ce Protocole doivent être appliquées, entre les Parties à ce Protocole, à des enquêtes ou procédures pénales spécifiques, concernant des infractions pénales liées à des systèmes et données informatiques (autrement dit les infractions couvertes par l'article 14 de la Convention, paragraphe 2, lettres a-b), ainsi qu'au recueil de preuves sous forme électronique d'une infraction pénale (Article 14 de la Convention, paragraphe 2.c). Comme expliqué aux paragraphes 141 et 243 du Rapport explicatif à la Convention, cela veut dire que lorsque l'infraction est commise par le biais d'un système informatique, ou lorsqu'une infraction qui n'a pas été commise par le biais d'un système informatique (par exemple un meurtre) implique des preuves électroniques, les pouvoirs, procédures et mesures de coopération créées par ce Protocole ont pour finalité de pouvoir être utilisées pour des enquêtes ou procédures pénales spécifiques.

34. Le paragraphe 2.1.b prévoit qu'entre les Parties au Premier Protocole qui sont Parties à ce Protocole, ce dernier s'applique aussi à des enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole. Les Parties à ce Protocole qui ne sont pas Partie au Premier Protocole ne prennent aucun engagement les obligeant à appliquer les termes du présent Protocole à ces infractions.

35. En vertu du paragraphe 2, il est demandé à chaque Partie de disposer d'une base juridique pour s'acquitter des obligations prévues dans le Protocole si ses traités, droit ou dispositifs ne contiennent pas déjà ces dispositions. Cela ne fait pas de dispositions explicitement discrétionnaires des dispositions contraignantes, et certaines dispositions prévoient des déclarations et des réserves. Certaines Parties peuvent ne pas avoir besoin de textes législatifs d'application pour mettre en œuvre les dispositions de ce Protocole.

Article 3 – Définitions

36. Le paragraphe 1 reprend les définitions fournies aux articles 1 (« Système informatique », « Données informatiques », « Fournisseur de services » et « Données relatives au trafic ») et 18, paragraphe 3, de la Convention (« Données relatives aux abonnés ») dans le présent Protocole. Les rédacteurs ont repris ces définitions de la Convention parce que ces termes sont utilisés dans le dispositif et le rapport explicatif de ce Protocole. Les rédacteurs ont également prévu que les explications fournies dans le rapport explicatif de la Convention et les notes d'orientation adoptés par le T-CY au sujet de ces termes s'appliqueraient également au présent Protocole.

37. Les définitions des infractions et des autres termes utilisés dans le texte de la Convention sont destinées à s'appliquer aux fins de la coopération entre les Parties au présent Protocole, et les définitions des infractions et des autres termes utilisés dans le texte du Premier Protocole sont destinées à s'appliquer aux fins de la coopération entre les Parties au Premier Protocole. Ainsi, par exemple, l'article 2, paragraphe 1, dispose que « les mesures que le présent Protocole énonce s'appliquent… « pour ce qui concerne les Parties à la Convention qui sont Parties au présent Protocole, à des enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques ». Par conséquent, lorsque la coopération au titre du

présent Protocole porte sur des infractions liées à la pornographie enfantine, la définition de la « pornographie enfantine » figurant à l'article 9, paragraphe 2, de la Convention s'applique, et la définition de « mineur » figurant à l'article 9, paragraphe 3, de la Convention. De même, pour ce qui concerne les Parties au Premier Protocole qui sont Parties au présent Protocole, la définition du « matériel raciste et xénophobe » de l'article 2 du Premier Protocole s'applique. Les Parties au présent Protocole qui ne sont pas Parties au Premier Protocole ne sont pas tenues d'appliquer les termes ou définitions énoncés dans le Premier Protocole.

38. Le paragraphe 2 de l'article 3 comprend des définitions supplémentaires qui s'appliquent au protocole et à la coopération au titre du protocole. Le paragraphe 2.a définit l'« autorité centrale » comme étant l'autorité ou les autorités désignées en vertu d'un traité d'entraide ou d'un arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, ou, à défaut, l'autorité ou les autorités désignées par une Partie aux termes de l'article 27, paragraphe 2.a, de la Convention. Le Protocole utilise les autorités centrales dans plusieurs articles pour que la coopération soit assurée par un moyen que les Parties mettent déjà en œuvre et qu'elles connaissent bien. Ainsi, les Parties qui ont conclu des traités d'entraide ou des arrangements reposant sur des législations uniformes ou réciproques sont tenues d'utiliser les autorités centrales désignées aux termes de ces traités ou arrangements. Lorsqu'aucun traité ou arrangement de ce type n'est en vigueur entre les Parties concernées, ces dernières sont tenues d'utiliser la même autorité centrale qu'elles utilisent actuellement en vertu des dispositions de l'article 27, paragraphe 2.a de la Convention. Tous les traités d'entraide ou arrangements reposant sur des législations uniformes ou réciproques n'utilisent pas l'expression « autorité centrale », mais les rédacteurs ont souhaité qu'il désigne les autorités de coordination désignées dans lesdits traités ou arrangements, quelle que soit la façon dont elles y sont dénommées.

39. Sauf disposition expresse du présent Protocole, le fait que les Parties mobilisent aux fins de ce dernier des autorités centrales mises en place à l'aide des moyens susvisés ne veut pas dire que d'autres dispositions de ces traités ou arrangements d'entraide s'appliquent.

40. La définition de l'« autorité compétente » énoncée au paragraphe 2.b est inspirée du paragraphe 138 du rapport explicatif de la Convention. Le présent Protocole utilisant fréquemment cette expression, cette définition a été insérée dans le dispositif pour en faciliter la consultation.

41. Le paragraphe 2.c définit l'« urgence » comme « une situation présentant un risque grave et imminent pour la vie ou la sécurité d'une personne physique ». Ce terme est utilisé dans les articles 10,12 et 9. Dans le présent Protocole, la définition de l'« urgence » est destinée à imposer un seuil nettement plus élevé que les « cas d'urgence » visés à l'article 25, paragraphe 3, de la Convention. Par ailleurs, cette définition a été élaborée de façon que les Parties puissent prendre en considération les différents contextes dans lesquels le terme est utilisé dans le présent Protocole tout en tenant compte des lois et politiques applicable dans chacune d'elles.

42. La définition d'une urgence se rapporte aux situations dans lesquelles le risque est grave et imminent, excluant ainsi les situations dans lesquelles le risque pour la vie ou la sécurité d'une personne appartient déjà au passé ou est négligeable, ou dans lesquelles peut exister un risque futur qui n'est pas imminent. Ces prescriptions relatives à la gravité et au caractère imminent tiennent au fait que les articles 9 et 10 imposent à la Partie requise comme à la Partie requérante l'obligation, qui exige de nombreux intervenants, de réagir de manière très accélérée en situation d'urgence, les demandes en urgence devant alors se voir accorder un rang de priorité plus élevé que d'autres cas qui, tout en étant importants, sont un peu moins urgents, même s'ils ont été soumis plus tôt. Les situations impliquant « un risque grave et imminent pour la vie ou la sécurité d'une personne physique » sont, par exemple, la prise d'otage, situation dans laquelle existe un risque crédible et imminent de décès, de blessure grave ou d'un autre préjudice comparable pour la victime; la persistance des abus sexuels auxquels un enfant est soumis; les scénarios immédiatement postérieurs à une attaque terroriste, dans lesquels les autorités cherchent à savoir avec qui les attaquants ont été en communication afin de déterminer si de nouvelles attaques sont

imminentes, et les menaces pour la sécurité d'infrastructures essentielles s'accompagnant d'un risque grave et imminent pour la vie ou la sécurité d'une personne physique.

43. Comme expliqué au paragraphe 4 de l'article 10 et au paragraphe 154 du rapport explicatif qui concerne l'article 9, une Partie requise déterminera, en vertu de ces articles, si une « urgence » existe, en appliquant la définition donnée dans le présent article.

44. Le paragraphe 2.d définit les « données à caractère personnel » comme « les informations relatives à une personne physique identifiée ou identifiable ». On entend par « personne physique identifiable » une personne qui peut être identifiée, directement ou indirectement, à partir, en particulier, d'un numéro d'identification ou d'un ou plusieurs facteurs propres à son identité physique, physiologique, mentale, économique, culturelle ou sociale. La définition des « données à caractère personnel » dans le présent protocole correspond à celle donnée par d'autres instruments internationaux, comme la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) telle que modifiée par son Protocole d'amendement (STCE n° 223), les Lignes directrices de 2013 de l'OCDE sur la protection de la vie privée, le Règlement général de protection des données et la directive « Police-Justice » de l'Union européenne, ainsi que la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (« Convention de Malabo »).

45. Une personne est considérée comme n'étant pas « identifiable » lorsque l'identification nécessiterait un temps, des efforts ou des ressources déraisonnables. Si certaines informations sont propres à une personne donnée et établissent donc par définition un lien avec cette personne, d'autres informations peuvent ne permettre une identification qu'en combinaison avec des informations identifiantes ou à caractère personnel supplémentaires. En conséquence, si l'indentification d'une personne par recoupement avec des informations supplémentaires de cette nature devait nécessiter un temps, des efforts ou des ressources déraisonnables, les informations dont il est question ne constituent pas des données à caractère personnel. Le fait qu'une personne physique puisse être identifiée ou soit identifiable, directement ou indirectement, dépend des circonstances propres à un contexte donné (et peut varier dans le temps avec les innovations technologiques ou autres).

46. Les exigences de protection des données fixées par le présent Protocole ne s'appliquent pas aux données qui n'ont pas de « caractère personnel », comme les informations anonymisées qui ne peuvent pas être réidentifiées sans y consacrer un temps, des efforts ou des ressources déraisonnables.

Article 4 – Langue

47. Cet article fournit un cadre pour les langues qui peuvent être utilisées lorsqu'on s'adresse aux Parties et aux fournisseurs de services ou autres entités en vertu du présent Protocole. Même lorsque, dans la pratique, les Parties sont en mesure de travailler dans des langues autres que leurs langues officielles, cette possibilité peut ne pas être prévue par le droit interne ou les traités. L'objectif de cet article est d'apporter plus de souplesse dans le cadre du présent Protocole.

48. Les traductions inexactes ou coûteuses des demandes d'entraide en matière de preuves électroniques sont constamment critiquées et constituent un problème qui doit être traité d'urgence. Cet obstacle sape les processus légitimes d'obtention de données et de protection de la sécurité publique. Les mêmes considérations s'appliquent en dehors de l'entraide judiciaire traditionnelle, par exemple lorsqu'une Partie transmet une injonction directement à un prestataire de services sur le territoire d'une autre Partie en vertu de l'article 7, ou demande de donner effet à une injonction en vertu de l'article 8. Les possibilités de traduction automatique devraient s'améliorer, mais elles sont actuellement insuffisantes. Pour ces raisons, le problème de la traduction a été mentionné à plusieurs reprises dans les propositions relatives aux articles à inclure dans ce Protocole.

49. La traduction de et vers des langues moins courantes est particulièrement problématique, car ces traductions peuvent retarder considérablement une demande ou être dans les faits impossibles à obtenir. Elles peuvent aussi être trompeuses au point d'être inutilisables et leur mauvaise qualité peut faire perdre du temps aux deux Parties. Toutefois, le coût et la difficulté des traductions incombent de manière disproportionnée aux Parties requérantes où des langues moins courantes sont parlées.

50. En raison de cette charge disproportionnée, un certain nombre de Parties non anglophones ont demandé que l'anglais soit obligatoire dans ce Protocole. Ils ont noté que l'anglais est une langue couramment utilisée par les principaux fournisseurs de services. En outre, à mesure que les données sont déplacées et stockées plus largement dans le monde et que de plus en plus de pays s'entraident, la traduction peut devenir encore plus lourde et peu pratique. Par exemple, deux Parties peuvent utiliser des langues moins courantes, être géographiquement éloignées et avoir peu de contacts. Si la Partie A a soudainement besoin de l'aide de la Partie B, il se peut qu'elle ne parvienne pas à trouver un traducteur pour la langue de la Partie B, ou qu'une traduction éventuelle soit moins intelligible que la traduction anglaise effectuée par des personnes non-anglophones. Les rédacteurs ont particulièrement souligné que, pour accélérer l'assistance, tous les efforts devraient être faits pour accepter, en particulier, les demandes d'urgence au titre du présent Protocole, en anglais ou dans une langue commune, plutôt que d'exiger une traduction dans la langue officielle de la Partie requise.

51. Les rédacteurs du Protocole ont conclu que l'anglais ne devrait pas être obligatoire dans le texte de ce Protocole. Certaines Parties ont des exigences en matière de langues officielles qui excluent un tel mandat; de nombreuses Parties partagent une langue commune et n'ont pas besoin de l'anglais; et, dans certaines Parties, les fonctionnaires en dehors des capitales sont moins susceptibles de pouvoir lire l'anglais mais sont souvent impliqués dans l'exécution des demandes.

52. Ainsi, le paragraphe 1 est formulé en termes de « langue acceptable pour la Partie requise ou la Partie à laquelle les actes sont notifiés en vertu de l'article 7 ». Cette Partie peut spécifier des langues acceptables - par exemple, des langues largement répandues comme l'anglais, l'espagnol ou le français - même si elles ne sont pas prévues dans sa législation ou ses traités nationaux.

53. Au paragraphe 1, les termes « demandes, injonctions et renseignements qui les accompagnent » désignent

a. en vertu de l'article 8, la demande (paragraphe 3), l'injonction (paragraphe 3.a), des renseignements à l'appui (paragraphe 3.b) et de toute instruction spéciale de procédure (paragraphe 3.c);
b. dans le cas des Parties qui exigent une notification en vertu de l'article 7, paragraphe 5, l'injonction (paragraphe 3), les renseignements à l'appui (paragraphe 4) et le résumé des faits (paragraphe 5.a).
c. en vertu de l'Article 9, la requête (paragraphe 3)

Le terme « demandes » renvoie également au contenu des demandes en vertu des articles 10,11 et 12, qui comprend la documentation qui fait partie de la demande.

54. Dans la pratique, certains pays peuvent être disposés à accepter des demandes et des injonctions dans une langue autre qu'une langue spécifiée dans le droit interne ou dans les traités. Aussi, une fois par an, le T-CY mènera une enquête informelle sur les langues acceptables pour les demandes et les injonctions. Les Parties peuvent modifier leurs renseignements en tout temps et l'ensemble des Parties seront informées de ces changements. Elles peuvent indiquer qu'elles n'acceptent que des langues spécifiques pour certaines formes d'assistance. Les résultats de cette enquête seront visibles pour toutes les Parties à la Convention, et pas seulement pour les Parties à ce Protocole.

55. Cette disposition pragmatique démontre l'extrême importance d'accélérer la coopération. Elle fournit une base conventionnelle permettant à une Partie d'accepter d'autres langues aux fins du présent Protocole.

56. Dans de nombreux cas, les Parties ont conclu des traités d'entraide judiciaire qui précisent la ou les langues dans lesquelles les demandes doivent être présentées en vertu de ces traités. Le présent article n'interfère pas avec les termes de ces traités ou autres accords entre les Parties. En outre, aux fins du présent Protocole, on s'attend à ce qu'« une langue acceptable pour la Partie requise ou la Partie à laquelle les actes sont notifiés en vertu de l'article 7 » comprenne toute langue ou toutes langues spécifiées par ces traités ou accords. Par conséquent, une Partie requérante devrait appliquer la langue spécifiée dans les traités d'entraide judiciaire ou autres accords aux demandes et notifications faites au titre du présent Protocole, à moins que la Partie requise ou à laquelle les actes sont notifiés n'indique qu'elle est également disposée à accepter ces demandes ou notifications dans d'autres langues.

57. Si une Partie est disposée à accepter d'autres langues, elle indiquera au T-CY qu'elle a l'intention d'accepter certaines ou toutes sortes de demandes ou de notifications d'injonctions au titre du présent Protocole dans une autre langue.

58. Le paragraphe 2 détermine la (les) langue(s) que la Partie émettrice utilise pour soumettre des injonctions ou des demandes et les renseignements connexes aux fournisseurs de services ou des entités fournissant des services d'enregistrement de noms de domaine sur le territoire d'une autre Partie aux fins des articles 6 et 7. Cette disposition vise à assurer une coopération rapide et une certitude accrue sans imposer une charge supplémentaire aux fournisseurs de services ou des entités fournissant des services de noms de domaine lorsqu'ils reçoivent des injonctions ou des demandes de données. La première option prévue au paragraphe 2.a indique que l'injonction ou la demande peut être présentée dans une langue dans laquelle le prestataire de services ou l'entité accepte habituellement des injonctions ou demandes nationales de ses propres autorités dans le cadre d'enquêtes spécifiques ou de procédures pénales (« procédure interne comparable »). Pour les Parties qui ont une ou plusieurs langues officielles, il s'agirait d'une de ces langues. La deuxième option, prévue au paragraphe 2.b, indique que si un prestataire de services ou l'entité accepte de recevoir des injonctions ou des demandes dans une autre langue, par exemple la langue de son siège, ces injonctions et les informations qui les accompagnent peuvent être soumises dans cette langue. En troisième lieu, le paragraphe 2.c prévoit que, lorsque l'injonction ou la demande et les informations qui l'accompagnent ne sont pas émises dans l'une des langues des deux premières options, elles sont accompagnées d'une traduction dans l'une de ces langues.

59. Au paragraphe 2, les termes « injonctions en vertu de l'article 7 et les demandes en vertu de l'article 6, et tout renseignement complémentaire » désignent:

– en vertu de l'article 6, la demande (paragraphe 3); et
– en vertu de l'article 7, l'ordonnance (paragraphe 3) et les informations complémentaires (paragraphe 4)

60. Lorsqu'une Partie a exigé une notification conformément à l'article 7, une Partie requérante doit être prête à envoyer l'injonction et tout renseignement qui l'accompagne dans une langue acceptable pour la Partie qui exige la notification, même si le fournisseur de services accepte d'autres langues.

61. Le T-CY s'efforcera également de recueillir de manière informelle des informations sur les langues dans lesquelles les injonctions et les demandes ainsi que les informations qui les accompagnent seront soumises aux prestataires de services et aux entités fournissant des services d'enregistrement de noms de domaine en vertu du paragraphe 2 de l'article 4 et en informera les Parties dans le cadre de l'enquête décrite au paragraphe 54 du Rapport explicatif, ci-dessus.

Chapitre II – Mesures de coopération renforcée

Section 1 – Dispositions générales applicables au Chapitre II

Article 5 – Principes généraux applicables au Chapitre II

62. Le paragraphe 1 de cet article précise que les Parties s'assurent la coopération « la plus large possible », conformément aux dispositions du Chapitre II et comme prévu à l'article 23 et à l'article 25, paragraphe 1, de la Convention. Ce principe fait obligation aux Parties de s'assurer une coopération étendue et de réduire au minimum les obstacles à la circulation rapide et fluide de l'information et des preuves entre pays.

63. Les paragraphes 2 à 5 organisent les sept mesures de coopération du présent Protocole en quatre sections distinctes qui suivent la première section, relative aux principes généraux. Ces sections portent sur les différents types de coopération visés: la section 2 couvre la coopération directe avec des entités privées, la section 3 concerne la coopération renforcée entre les autorités pour la divulgation de données stockées, la section 4 porte sur l'entraide en cas d'urgence et la section 5 conclut par les dispositions internationales régissant la coopération en l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées. Elles sont aussi structurées de manière globalement progressive, allant des formes d'assistance souvent souhaitées dans les premiers stades d'une enquête – pour obtenir la divulgation de l'enregistrement de noms de domaine et informations relatives aux abonnés – aux demandes de données relatives au trafic puis aux données relatives au contenu, suivies des vidéoconférences et des équipes communes d'enquête, qui sont souvent les formes d'assistance recherchées à un stade plus avancée d'une enquête.

64. Cette section consacrée aux principes généraux indique clairement à quel point chaque mesure est affectée ou non par l'existence d'un traité d'entraide ou d'un arrangement reposant sur des législations uniformes ou réciproques en vigueur entre les Parties concernées, c'est-à-dire entre la Partie requérante et la Partie requise dans le cas de la coopération interétatique ou la Partie demandant les informations et la Partie sur le territoire de laquelle est située l'entité privée qui est en possession de ces informations ou qui en a le contrôle, pour la coopération directe en vertu des articles 6 et 7. On entend par « arrangement sur la base de législations uniformes ou réciproques » les mécanismes « tel que le système de coopération instauré entre les pays nordiques, qui est également reconnu par la Convention européenne d'entraide judiciaire en matière pénale (article 25, paragraphe 4), et le système instauré entre les membres du Commonwealth » (voir le paragraphe 263 du Rapport explicatif à la Convention). Les mesures prévues aux sections 2 à 4 de ce chapitre s'appliquent, que les Parties concernées soient ou non mutuellement liées par un accord d'entraide ou un arrangement applicable reposant sur des législations uniformes ou réciproques. Les dispositions de la section 5 relatives à la coopération internationale s'appliquent uniquement en l'absence d'un tel accord ou d'un tel arrangement, sauf dispositions contraires.

65. Comme décrit au paragraphe 2 de cet article, la section 2 de ce chapitre se compose de l'article 6, intitulé « Demande d'informations concernant l'enregistrement d'un nom de domaine », et de l'article 7, intitulé « Divulgation de données relatives aux abonnés ». Il s'agit des articles dits de « coopération directe », qui permettent aux autorités compétentes d'une Partie de s'engager directement avec des entités privées - c'est-à-dire avec des entités fournissant des services d'enregistrement de noms de domaine à l'article 6, et avec des prestataires de services à l'article 7 - aux fins d'enquêtes ou de procédures pénales spécifiques. L'article 2 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre la Partie qui recherche les informations et la Partie sur le territoire de laquelle se trouve l'entité privée en possession ou en charge de ces informations.

66. Comme décrit au paragraphe 3 de cet article, la section 3 de ce chapitre se compose de l'article 8, intitulé « Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données », et de l'article 9, intitulé « Divulgation accélérée de données informatiques stockées en situation d'urgence ». Il s'agit de mesures de « coopération internationale renforcée entre autorités », c'est-à-dire qu'elles prévoient une coopération entre autorités compétentes, mais d'une nature différente de la coopération internationale traditionnelle. La section 3 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les parties requérante et requise.

67. Comme décrit au paragraphe 4 du présent article, la section 4 du présent chapitre se compose de l'article 10, intitulé « Entraide d'urgence ». Bien que l'entraide d'urgence soit une disposition d'entraide, elle constitue un outil de coopération important pour les situations d'urgence qui n'est pas expressément prévu dans de nombreux traités d'entraide. Par conséquent, les rédacteurs ont décidé que cette section devait s'appliquer, qu'il existe ou non un accord ou un arrangement d'entraide applicable, sur la base de la législation uniforme ou réciproque en vigueur entre les Parties concernées. En ce qui concerne les procédures qui régissent l'entraide en cas d'urgence, il existe deux possibilités. Lorsque les Parties concernées sont mutuellement liées par un accord d'entraide applicable, ou un arrangement d'entraide applicable sur la base d'une législation uniforme ou réciproque, la section 4 est complétée par les dispositions de cet accord, à moins que les Parties concernées ne décident mutuellement d'appliquer certaines dispositions de la Convention à la place. Voir l'article 10, paragraphe 8. Lorsque les Parties concernées ne sont pas mutuellement liées par un tel accord ou arrangement, les Parties appliquent certaines procédures énoncées aux articles 27 et 28 de la Convention (régissant l'entraide en l'absence de traité). Voir l'article 10, paragraphe 7.

68. Comme décrit au paragraphe 5 du présent article, la section 5 du présent chapitre se compose de l'article 11, intitulé « Vidéoconférence », et de l'article 12, intitulé « Équipes communes d'enquête et enquêtes communes ». Ces dispositions sont des mesures de coopération internationale, qui ne s'appliquent que lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base d'une législation uniforme ou réciproque en vigueur entre les Parties requérante et requise. Ces mesures ne s'appliquent pas lorsqu'un tel traité ou arrangement existe, sauf que l'article 12, paragraphe 7 s'applique qu'un tel traité ou arrangement existe ou non. Toutefois, les Parties concernées peuvent décider mutuellement d'appliquer les dispositions de la section 5 en lieu et place d'un tel traité ou arrangement existant, à moins que cela ne soit interdit par les termes du traité ou de l'arrangement.

69. Le paragraphe 6 prend pour modèle l'article 25 paragraphe 5 de la Convention, et le paragraphe 259 du rapport explicatif de la Convention est donc également valable ici: « Lorsque la Partie requise est autorisée à exiger la double incrimination comme condition de l'octroi de l'entraide [...] la double incrimination est réputée présente si le comportement à l'origine de l'infraction pour laquelle l'entraide est demandée constitue également une infraction pénale en vertu des lois de la Partie requise, même si ses lois classent l'infraction dans une catégorie différente ou utilisent une terminologie différente pour la désigner. Cette disposition a été jugée nécessaire afin de s'assurer que les Parties requises n'adoptent pas un critère trop rigide lorsqu'elles appliquent la double incrimination. Compte tenu des différences entre les systèmes juridiques nationaux, des variations dans la terminologie et la catégorisation des comportements criminels sont inévitables. Si le comportement constitue une infraction pénale dans les deux systèmes, ces différences techniques ne devraient pas entraver l'assistance. Au contraire, dans les affaires où le critère de la double incrimination est applicable, il doit être appliqué de manière souple afin de faciliter l'octroi de l'assistance. »

70. Le paragraphe 7 prévoit que « [l]es dispositions du présent chapitre ne restreignent pas la coopération entre les Parties, ou entre les Parties et les prestataires de services ou d'autres entités, par le biais d'autres accords, arrangements, pratiques ou de la loi nationale, applicables. » Cela signifie que le Protocole n'élimine ni ne restreint aucune coopération entre les Parties ou entre les

Parties et des entités privées, qui est par ailleurs disponible - que ce soit par le biais d'accords, d'arrangements, de la loi nationale, applicables ou même de pratiques informelles. Les rédacteurs avaient l'intention d'élargir, et non de restreindre, les outils disponibles dans la boîte à outils du praticien de l'application des lois pour obtenir des informations ou des preuves dans le cadre d'enquêtes ou de procédures pénales spécifiques. Les rédacteurs ont reconnu que dans certaines situations, les mécanismes existants, tels que l'entraide judiciaire, peuvent être les mieux utilisés par un praticien. Cependant, dans d'autres situations, les outils créés par ce Protocole peuvent être plus efficaces ou préférables. Par exemple, si une autorité compétente a besoin de données relatives au contenu de manière non urgente, elle choisira probablement d'utiliser une demande d'entraide traditionnelle en vertu d'un traité bilatéral ou de l'article 27 de la Convention, selon le cas, car le Protocole ne contient pas de dispositions permettant d'obtenir des données relatives au contenu de manière non urgente. Mais si elle avait besoin d'informations sur les abonnés, elle pourrait choisir d'utiliser l'article 7 du Protocole pour émettre un ordre directement à un fournisseur de services.

71. Enfin, un certain nombre de dispositions du chapitre II et d'autres dispositions du Protocole permettent d'imposer des limitations ou des conditions d'utilisation, telles que la confidentialité. Lorsque, conformément aux dispositions du Protocole, la réception des preuves ou des informations recherchées est soumise à une telle limitation ou condition d'utilisation, des exceptions ont été reconnues par les négociateurs et sont implicites dans le texte. Premièrement, en tant que mesure de protection des droits de l'homme et des libertés conformément à l'article 13, en vertu des principes juridiques fondamentaux de nombreux États, si des éléments fournis à la Partie destinataire sont considérés par celle-ci comme étant à décharge d'une personne accusée, ils doivent être divulgués à la défense ou à une autorité judiciaire. Ce principe est sans préjudice du texte de l'article 12, paragraphe 6.b et du Rapport explicatif, paragraphe 275 qui peuvent être appliqués lorsque les Parties ont mis en place une équipe commune d'enquête. Il est entendu par les rédacteurs que, dans de tels cas, la Partie destinataire notifie la Partie transférante avant la divulgation et, si cette dernière le demande, consulte la Partie transférante. Deuxièmement, lorsqu'une limitation d'utilisation a été imposée à l'égard de matériel reçu en vertu du présent Protocole et dont l'utilisation est prévue au cours d'un procès, le procès (y compris les divulgations au cours des procédures judiciaires préalables au procès) est normalement une procédure publique. Une fois rendu public lors du procès, le matériel tombe dans le domaine public. Dans ces situations, il n'est pas possible de garantir la confidentialité de l'enquête ou de la procédure pour laquelle le matériel a été demandé. Ces exceptions sont similaires aux exceptions liées à l'application de l'article 28, paragraphe 2, de la Convention, comme expliqué au paragraphe 278 du Rapport explicatif de la Convention. Enfin, le matériel peut être utilisé à d'autres fins lorsque le consentement préalable d'une Partie transférante a été obtenu.

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

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

72. Cet article établit une procédure qui prévoit la coopération directe entre les autorités d'une Partie et une entité prestataire de services d'enregistrement de noms de domaine, située sur le territoire d'une autre Partie, pour obtenir des informations sur l'enregistrement de noms de domaine sur Internet. Comme pour l'article 7, la procédure s'appuie sur les conclusions du Groupe sur les preuves dans le nuage du Comité de la Convention sur la cybercriminalité, reconnaissant l'importance que revêt un accès transfrontalier rapide à des preuves électroniques pour des enquêtes ou des procédures pénales spécifiques, au vu des difficultés que posent les procédures existantes pour l'obtention de preuves électroniques.

73. La procédure reconnaît également le modèle actuel de gouvernance internet qui repose sur l'élaboration de politiques multi-parties prenantes basées sur le consensus. Ces politiques sont

normalement fondées sur le droit des contrats. La procédure visée dans cet article entend compléter ces politiques pour les objectifs de ce Protocole, autrement dit aux fins d'enquêtes ou de procédures pénales spécifiques. L'obtention des données d'enregistrement d'un nom de domaine constitue souvent une première étape indispensable pour de nombreuses enquêtes criminelles, et pour déterminer où adresser des demandes de coopération internationale.

74. De nombreuses formes de cybercriminalité sont facilitées par le fait que des criminels créent et exploitent des domaines à des fins malveillantes et illicites. Ainsi, un nom de domaine peut être utilisé comme plateforme pour disséminer des maliciels, des botnets, mener des activités de phishing et autres activités de même genre, se livrer à la fraude, ou encore à la diffusion de matériels de pédopornographie, pour ne citer que quelques exemples. L'accès aux informations sur la personne physique ou morale qui a enregistré le domaine (le « déclarant ») est donc critique pour identifier un suspect dans une enquête ou procédure pénale spécifique. Au départ, les données d'enregistrement des noms de domaine étaient accessibles à tous; maintenant, certaines parties de l'information sont d'accès restreint, ce qui a des répercussions sur les missions de politique publique des services judiciaires et répressifs.

75. Les informations concernant l'enregistrement de noms de domaine sont détenues par des entités prestataires de services d'enregistrement de noms de domaine. Ces dernières prennent la forme d'organisations vendant des noms de domaine au public (les « registraires ») ainsi que d'opérateurs régionaux ou nationaux de registres qui conservent des bases de données officielles (les « registres ») de tous les noms de domaine enregistrés pour un domaine de premier niveau et qui acceptent des demandes d'enregistrement. Dans certains cas, ces informations peuvent constituer des données à caractère personnel et être protégées en vertu des dispositions de protection des données dans le droit interne de la Partie sur le territoire de laquelle se trouve l'entité concernée fournissant des services d'enregistrement de noms de domaine (registraire ou registre) ou la personne à laquelle se réfèrent les données.

76. L'article 6 entend donner un cadre effectif et efficient d'obtention d'informations pour identifier ou contacter le registrant d'un nom de domaine. Les modalités de sa mise en œuvre dépendent des considérations légales et politiques des différentes Parties. Cet article entend compléter les politiques et pratiques actuelles et futures de gouvernance internet.

Paragraphe 1

77. En vertu du paragraphe 1, chaque Partie adopte les mesures nécessaires pour habiliter ses autorités compétentes à adresser des demandes directement à une entité prestataire de services d'enregistrement de noms de domaine située sur le territoire d'une autre Partie, autrement sans demander aux autorités compétentes sur le territoire où l'entité est située d'intervenir en tant qu'intermédiaire. Le paragraphe 1 donne aux Parties une certaine flexibilité par rapport au format dans lequel les demandes sont présentées, car le format dépend des considérations juridiques et politiques respectives des Parties. Une Partie peut utiliser les procédures disponibles dans son système de loi nationale, y compris l'émission d'une injonction; toutefois, aux fins du présent article, une telle demande est traitée comme une demande non contraignante. La forme de la demande ou les effets qu'elle produit en vertu du droit interne de la Partie requérante n'affecterait donc pas le caractère volontaire de la coopération internationale au titre du présent article et, si l'entité ne divulgue pas les informations recherchées, le paragraphe 5 serait applicable.

78. Le libellé du paragraphe 1 est suffisamment générique pour reconnaître qu'une telle demande peut aussi être émise et les informations obtenues via une interface, un portail ou autre outil technique mis à disposition par des organisations. Ainsi, une organisation peut fournir une interface ou un outil de recherche pour faciliter ou accélérer la divulgation d'informations sur l'enregistrement d'un nom de domaine à la suite d'une demande. En revanche, plutôt que de viser un portail ou interface spécifiques, l'article utilise des termes neutres du point de vue technologique pour permettre une adaptation à l'évolution en la matière.

79. Comme prévu dans l'article 2, une demande en vertu du paragraphe 1 peut être émise uniquement aux fins d'enquêtes ou procédures pénales spécifiques. L'expression « autorités compétentes » est définie sous l'Article 3, paragraphe 2.b et « désigne une autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de mesures au titre du présent protocole ». Une « entité prestataire de services d'enregistrement de noms de domaine » renvoie actuellement aux registraires et registres. Pour prendre en compte la situation actuelle et dans le même temps permettre une adaptation pour le cas où les modèles économiques et l'architecture de l'Internet changent au fil du temps, cet article utilise l'expression plus générique de « entité prestataire de services d'enregistrement de noms de domaine».

80. Si les informations pour identifier ou contacter le registrant d'un nom de domaine sont souvent stockées par des entités prestataires de services génériques d'enregistrement de noms de domaine dans le monde entier, ce qu'on appelle des « domaines génériques de premier niveau (« generic top level domains » ou gTLDs), les Parties ont reconnu que des services plus spécifiques en matière d'enregistrement de noms de domaine liés à des entités nationales ou régionales (les domaines nationaux de premier niveau, « country-code top level domains » ou ccTLDs)) peuvent aussi être enregistrés par des personnes morales ou physiques dans d'autres pays et peuvent aussi être utilisées par des criminels. Cet article ne se limite donc pas aux entités prestataires de gTLD, car les deux types de services concernant l'enregistrement de noms de domaine – ou les futurs types de services de ce genre – peuvent être utilisés pour perpétrer des actes de cybercriminalité.

81. L'expression « Informations … pour identifier ou contacter le registrant d'un nom de domaine » renvoie aux informations qui étaient auparavant publiquement accessibles par des outils de recherche connus sous l'acronyme WHOIS, par exemple le nom, l'adresse physique, l'adresse électronique et le numéro de téléphone d'un registrant. Certaines Parties peuvent considérer ces informations comme un sous-ensemble des informations relatives aux abonnés au sens de l'article 18.3 de la Convention. Les informations d'enregistrement de noms de domaine sont des informations de base qui ne permettraient pas de tirer des conclusions précises concernant la vie privée et le modus vivendi de quelqu'un. Leur divulgation peut donc être moins intrusive que celle d'autres catégories de données.

Paragraphe 2

82. Le paragraphe 2 fait obligation à chaque Partie d'adopter des mesures pour permettre à des entités prestataires de services d'enregistrement de noms de domaine établies sur son territoire de divulguer ces informations en réponse à une demande visée au paragraphe 1, sous réserve des conditions raisonnables prévues par la loi nationale, qui, dans certaines Parties, peuvent inclure des conditions découlant des lois sur la protection des données à caractère personnel. En même temps, l'article 14 limite la possibilité de refuser des transferts de données en vertu des règles de protection des données pour les transferts internationaux, et les facteurs du paragraphe 82 ont été inclus pour faciliter le traitement en vertu des règles de protection des données. Ces mesures devraient faciliter la divulgation des données demandées de manière rapide et efficace dans toute la mesure du possible.

83. Cet article ne fait pas obligation aux Parties d'adopter des textes législatifs contraignant ces entités à répondre à une demande émanant d'une autorité d'une autre Partie. Ainsi, l'entité offrant des services d'enregistrement de noms de domaine peut avoir besoin de déterminer si elle doit divulguer les informations recherchées. Le Protocole contribue à cette détermination en fournissant des garanties qui devraient faciliter la capacité des entités de répondre sans difficulté aux demandes au titre du présent article, telles que:

– le Protocole fournit ou oblige les Parties à fournir une base juridique pour les demandes;

- cet article exige que la demande provienne d'une autorité compétente (article 6, paragraphes 1 et 3.a et paragraphe 79 et 84 de ce Rapport explicatif);
- le Protocole prévoit qu'une demande est faite aux fins d'enquêtes ou de procédures pénales spécifiques 2;
- cet article exige que la demande contienne une déclaration selon laquelle le besoin de l'information découle de sa pertinence pour une enquête ou une procédure pénale spécifique et que l'information ne soit utilisée que pour cette enquête ou procédure pénale spécifique. (article 6, paragraphe 3.c);
- le protocole prévoit des garanties pour le traitement des données à caractère personnel divulguées et transférées conformément à ces demandes au titre de l'article 14;
- les informations à divulguer sont limitées et ne permettraient pas de tirer des conclusions précises concernant la vie privée des personnes visées;
- il est possible d'escompter des entités qu'elles coopèrent ou de les y obliger en vertu d'arrangements contractuels avec l'ICANN.

Paragraphe 3

84. Le paragraphe 3 de cet article spécifie les informations qui, à minima, doivent être fournies par une autorité formulant une demande en vertu du paragraphe 1 de cet article. Ces informations sont particulièrement pertinentes pour l'exécution de la demande par l'entité prestataire de services d'enregistrement de noms de domaine. La demande devra inclure:

a. la date d'émission ainsi que l'identité et les coordonnées de l'autorité compétente qui émet la demande (paragraphe 3.a) (voir paragraphe 79 du Rapport explicatif).
b. le nom de domaine au sujet duquel les informations sont demandées et une liste détaillée des informations recherchées, y compris les éléments de données spécifiques tels que le nom, l'adresse physique, l'adresse électronique ou le numéro de téléphone du registrant (paragraphe 3.b);
c. une déclaration selon laquelle la demande est émise conformément au présent Protocole; par cette déclaration, la Partie atteste que la demande est conforme aux dispositions du Protocole (paragraphe 3.c). La Partie émettrice confirme également dans cette déclaration qu'elle a « besoin » de ces informations du fait de leur pertinence pour une enquête ou procédure pénale spécifique et que les informations ne seront utilisées que pour cette enquête ou procédure pénale spécifique. Si les Parties sont des pays européens, le critère du « besoin de ces informations » – autrement dit les informations doivent être nécessaires et proportionnées – pour une enquête ou procédure pénale devrait découler des principes de la Convention du Conseil de l'Europe de 1950 relative à la protection des droits de l'homme et des libertés fondamentales, de sa jurisprudence applicable et du droit et de la jurisprudence internes aux Parties. Il découle de ces sources que la compétence ou la procédure devraient être proportionnelles à la nature et aux circonstances d'une infraction (voir paragraphe 146 du Rapport explicatif de la Convention). D'autres Parties appliqueront les principes de leur droit interne adaptés tels que le principe de pertinence (en d'autres termes, la preuve recherchée par une demande doit être pertinente pour l'enquête ou les poursuites. Les parties devraient éviter les demandes générales de divulgation d'informations concernant les noms de domaine, à moins qu'elles ne soient nécessaires pour l'enquête ou la procédure pénale spécifique;
d. l'échéance et les modalités de divulgation des informations et autres instructions procédurales spéciales (paragraphe 3.d). L'expression « Instructions procédurales spéciales » entend inclure toute demande de confidentialité, notamment une demande de non-divulgation de la demande au registrant ou à un autre tiers. Si la confidentialité est demandée pour éviter une divulgation prématurée de l'affaire, cela devrait figurer dans la demande. Dans certaines Parties, la confidentialité de la demande sera appliquée automatiquement par dispositions légales, alors que dans d'autres, ce ne sera pas nécessairement le cas. C'est pourquoi, là où la confidentialité est nécessaire, les Parties sont encouragées à examiner les informations publiquement accessibles et demander des conseils aux autres Parties concernant le droit

applicable ainsi que des politiques des entités prestataires de services d'enregistrement de noms de domaine concernant l'information d'un abonné/registrant avant de soumettre à l'entité une demande en vertu du paragraphe 1. En outre, les instructions procédurales spéciales peuvent prévoir la spécification du canal de transmission le plus adapté aux besoins de l'autorité.

85. Le paragraphe 3 ne prévoit pas d'obligation d'inclure un descriptif des faits dans la demande, étant donné que ces informations sont confidentielles dans la plupart des enquêtes criminelles et ne peuvent être divulguées à une personne non habilitée. Toutefois, l'entité qui reçoit une demande au titre du présent article peut avoir besoin de certaines informations supplémentaires qui lui permettraient de prendre une décision positive concernant la demande. Par conséquent, l'entité peut demander un complément d'informations lorsque, sans celles-ci, elle n'est pas en mesure d'exécuter la demande.

Paragraphe 4

86. L'objectif du paragraphe 4 est d'encourager l'utilisation de moyens électroniques lorsque ceux-ci sont acceptables pour l'entité fournissant des services d'enregistrement de noms de domaine, car ce sont presque toujours les moyens de communication les plus efficaces et les plus rapides. En conséquence, si cela est acceptable pour l'entité fournissant des services d'enregistrement de noms de domaine, une Partie peut soumettre une demande à l'entité sous forme électronique, par exemple en utilisant le courrier électronique, les portails électroniques ou d'autres moyens. Bien que l'on suppose que les entités préfèrent recevoir les demandes sous cette forme, il ne s'agit pas d'une exigence. Comme le prévoient d'autres articles du présent protocole autorisant les ordonnances ou les demandes sous forme électronique (tels que les articles 7, 8 et autres), des niveaux appropriés de sécurité et d'authentification peuvent être exigés. Les parties et les entités peuvent décider elles-mêmes si des voies ou des moyens de transmission et d'authentification sécurisés sont disponibles ou si des protections de sécurité spéciales (y compris le cryptage) peuvent être nécessaires dans un cas sensible particulier.

Paragraphe 5

87. Bien que cette disposition relève des « demandes » et non des « injonctions » contraignantes pour la divulgation de données d'enregistrement de noms de domaine, il est escompté que l'entité destinataire de la demande sera en mesure de divulguer les informations demandées en vertu de cette disposition, une fois les conditions applicables satisfaites. Si l'entité ne divulgue pas les informations demandées, d'autres mécanismes pourraient être envisagés pour les obtenir, en fonction des circonstances. Le paragraphe 5 prévoit donc une consultation entre les Parties concernées pour obtenir des informations supplémentaires et déterminer quels mécanismes peuvent être activés. Afin de faciliter les consultations, le paragraphe 5 dispose également qu'une Partie requérante peut demander des informations complémentaires à une entité. Les entités sont encouragées à motiver leur refus de divulguer les données demandées en réponse à une telle demande.

Paragraphe 6

88. Le paragraphe 6 impose que les Parties désignent, au moment de la signature de ce Protocole ou du dépôt de leur instrument de ratification, d'acceptation ou d'approbation, ou à tout autre moment, une autorité aux fins de la consultation prévue au paragraphe 5. La désignation d'un point de contact dans l'État partie où est située l'entité aidera la Partie requérante à déterminer rapidement les mesures auxquelles il est possible de recourir pour obtenir les données souhaitées dans le cas où l'entité refuse d'accéder à une requête directe adressée en vertu de cet article.

Paragraphe 7

89. Le paragraphe 7 est explicite et dispose que le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités désignées en vertu du paragraphe 6 et que chaque Partie veille à ce que les données qu'elle a fournies pour le registre soient correctes à tout moment.

Article 7 – Divulgation des informations sur les abonnés

90. Cet article établit une procédure prévoyant la coopération directe entre les autorités d'une Partie et un fournisseur de services sur le territoire d'une autre Partie en vue d'obtenir des données relatives aux abonnés. Cette procédure repose sur les conclusions du Groupe de travail du Comité de la Convention sur les preuves dans le nuage et sur la Note d'orientation du Comité relative à l'article 18 de la Convention, reconnaissant l'importance de l'accès transfrontalier en temps opportun aux éléments de preuve électroniques dans les enquêtes ou les procédures pénales spécifiques, eu égard aux difficultés que posent les procédures existantes pour obtenir des éléments de preuve électroniques auprès des fournisseurs de services dans d'autres pays.

91. Un nombre croissant d'enquêtes ou de procédures pénales nécessitent aujourd'hui d'avoir accès à des éléments de preuve électroniques détenus par des fournisseurs de services dans d'autres pays. Même dans le cas d'infractions strictement internes par nature – c'est-à-dire lorsque la victime et l'auteur se trouvent tous deux dans le pays où a lieu l'infraction, de même que l'autorité chargée de l'enquête – les éléments de preuve électroniques peuvent être détenus par un fournisseur de services sur le territoire d'un autre pays. Dans bien des situations, les autorités qui enquêtent sur une infraction peuvent être amenées à recourir à des procédures de coopération internationale, comme l'entraide judiciaire, qui ne permettent pas toujours d'obtenir une aide rapide ou suffisamment efficace pour répondre aux besoins de l'enquête ou de la procédure en raison du volume des demandes de preuves électroniques, qui ne cesse d'augmenter.

92. Les données relatives aux abonnés sont les informations les plus fréquemment recherchées dans les enquêtes pénales relatives à la cybercriminalité et à d'autres types d'infractions qui nécessitent l'obtention de preuves électroniques. Elles indiquent l'identité d'un abonné à un service particulier, son adresse et des informations similaires visées à l'article 18.3 de la Convention. Ces données ne permettent pas de tirer des conclusions précises sur la vie privée et les habitudes quotidiennes des personnes concernées, ce qui signifie que leur divulgation peut être moins intrusive que celle d'autres catégories de données.

93. Les données relatives aux abonnés sont définies à l'article 18, paragraphe 3, de la Convention (incorporées à l'article 3, paragraphe 1, de ce Protocole) selon lequel « toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a. le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b. l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ; c. toute autre information sur le site d'installation des équipements de communication, disponible sur la base du contrat ou de l'arrangement de service...» (voir aussi le Rapport explicatif de la Convention, paragraphes 177-183). Les informations nécessaires à l'identification d'un abonné à un service peuvent inclure certaines données relatives à l'adresse IP (Internet Protocol) – l'adresse IP utilisée au moment de la création du compte, l'adresse IP utilisée la plus récemment pour se connecter au service ou les adresses IP utilisées pour se connecter à un moment précis, par exemple. Dans certains États parties, ces informations sont traitées comme des données relatives au trafic pour diverses raisons, notamment parce qu'elles sont considérées comme ayant trait à la transmission d'une communication. En conséquence, le paragraphe 9.b prévoit une possibilité de réserve pour certaines Parties.

94. Bien que l'article 18 de la Convention traite déjà de certains aspects de la nécessité d'un accès rapide et effectif aux preuves électroniques détenues par des fournisseurs de services, il n'apporte pas à lui seul une solution complète à ce problème, étant donné qu'il s'applique dans des circonstances plus limitées. Plus précisément, cet article s'applique lorsqu'un fournisseur de services se trouve « sur le territoire » de la Partie émettrice (voir article 18, paragraphe 1.a de la Convention) ou « offre ses prestations » dans la Partie émettrice (voir article 18, paragraphe 1.b). Compte tenu des limites de l'article 18 et des difficultés qui se posent dans la mise en œuvre de l'entraide judiciaire, il a été jugé important d'établir un mécanisme complémentaire qui permettrait un accès transfrontalier plus effectif aux informations nécessaires aux enquêtes ou aux procédures pénales spécifiques. En conséquence, le champ d'application de cet article est plus étendu que celui de l'article 18 de la Convention, car il permet à une Partie d'adresser certaines injonctions aux fournisseurs de services sur le territoire d'une autre Partie. Les Parties ont reconnu que, bien que de telles injonctions adressées directement par les autorités d'une Partie à des fournisseurs de services situés dans une autre Partie soient souhaitables pour favoriser un accès rapide et efficace aux données requises, il ne devrait pas être permis à une Partie d'employer tous les mécanismes d'exécution prévus par son droit interne pour faire exécuter ces injonctions. Pour cette raison, l'exécution de ces injonctions, dans les cas où le fournisseur ne divulgue pas les données relatives aux abonnés demandées, est limitée à la manière énoncée au paragraphe 7 de cet article. Cette procédure prévoit des garanties permettant de tenir compte des exigences particulières découlant d'une coopération directe entre les autorités d'une Partie et les fournisseurs de services se trouvant sur le territoire d'une autre Partie.

95. Comme indiqué à l'article 5, paragraphe 7, le présent article est sans préjudice de la capacité des Parties à exécuter les injonctions adressées en application de l'article 18 ou de toute autre manière autorisée par la Convention, et ne porte pas non plus atteinte à la coopération (y compris une coopération spontanée) entre Parties, ou entre Parties et fournisseurs de services, au moyen d'autres accords, dispositions, pratiques ou lois nationales.

Paragraphe 1

96. Le paragraphe 1 impose aux Parties de conférer aux autorités compétentes les pouvoirs nécessaires pour adresser à un fournisseur de services sur le territoire d'une autre Partie une injonction de produire des données relatives aux abonnés. Cette injonction ne peut être émise qu'aux fins d'obtention de données spécifiées et stockées relatives à des abonnés.

97. Le paragraphe 1 prévoit également l'obligation selon laquelle les injonctions ne peuvent être émises et adressées que dans le cadre d' « enquêtes ou de procédures pénales spécifiques » menées par le pays émetteur, au sens de l'article 2 de ce Protocole. En outre, les injonctions ne peuvent être émises que pour obtenir des informations « nécessaires » à l'enquête ou à la procédure en question. Pour les pays européens, les informations requises – qui doivent être nécessaires et proportionnées – pour une enquête ou une procédure pénale doivent respecter les principes issus de la Convention 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. D'après ces principes, les pouvoirs ou les procédures doivent être proportionnelles à la nature et aux circonstances de l'infraction (voir paragraphe 146 du Rapport explicatif de la Convention sur la cybercriminalité). D'autres Parties mettront en œuvre des principes connexes de leur droit interne, comme les principes de pertinence (l'élément de preuve demandé au moyen de l'injonction doit être pertinent pour l'enquête ou les poursuites engagées) et de limitation de la portée des injonctions de produire des données relatives aux abonnés, pour éviter qu'elle soit trop large. Cette restriction souligne le principe déjà énoncé à l'article 2 de ce Protocole et au paragraphe 1 de cet article, qui limite la mesure à des enquêtes et procédures pénales spécifiques, selon lequel ces dispositions ne peuvent être utilisées pour obtenir la communication de données en masse (voir également le Rapport explicatif, paragraphe 182 de la Convention)..

98. Comme défini au paragraphe 2.b de l'article 3, l'expression « autorités compétentes » désigne une autorité judiciaire, administrative ou autre autorité chargée de l'application de la loi qui est habilitée par le droit interne à ordonner, autoriser ou entreprendre l'exécution des mesures prévues par le présent protocole. La même approche est prévue aux fins de la procédure de coopération directe visée dans cet article. En conséquence, l'ordre juridique national d'une Partie détermine quelle autorité est considérée comme une autorité compétente pour adresser une injonction. Bien que la Partie émettrice définisse laquelle de ses autorités est habilitée à émettre l'injonction, cet article prévoit une garantie au paragraphe 5, selon lequel la Partie destinataire peut exiger qu'une autorité désignée examine les injonctions adressées en application de cet article et ait la possibilité de mettre fin à la coopération directe, comme décrit plus loin.

99. Dans cet article, l'expression « fournisseur de services sur le territoire d'une autre Partie » nécessite que le fournisseur de services soit physiquement présent sur le territoire de l'autre Partie. En vertu de cet article, le simple fait, par exemple, qu'un fournisseur de services ait établi une relation contractuelle avec une entreprise dans un État partie, mais que le fournisseur de services lui-même ne soit pas physiquement présent sur le territoire de cette Partie, ne permettrait pas de considérer que le fournisseur de services se trouve « sur le territoire » de cette Partie. Le paragraphe 1 exige, en outre, que les données soient en la possession ou sous le contrôle du fournisseur de services.

Paragraphe 2

100. Aux termes du paragraphe 2 de cet article, les Parties sont tenues d'adopter toutes les mesures nécessaires pour que les fournisseurs de services sur leur territoire répondent à une injonction adressée par une autorité compétente dans une autre Partie, conformément au paragraphe 1. Compte tenu des différences entre les systèmes juridiques nationaux, les Parties peuvent mettre en œuvre des mesures différentes pour appliquer une procédure permettant d'établir une coopération directe de manière efficace et efficiente. Ces dispositions peuvent aller de l'élimination des obstacles juridiques auxquels se heurtent les fournisseurs de services pour répondre à une injonction, à la mise en place d'une base positive obligeant les fournisseurs de services à répondre à une injonction adressée par une autorité d'un autre État partie de manière efficace et efficiente. Chaque Partie doit veiller à ce que les fournisseurs de services puissent se conformer en toute légalité aux injonctions visées par cet article d'une manière qui garantisse la sécurité juridique, de sorte que les fournisseurs de services ne voient pas leur responsabilité juridique engagée du seul fait qu'ils se sont conformés de bonne foi à une injonction adressée en vertu du paragraphe 1 et pour laquelle une Partie a déclaré qu'elle est émise en application de ce Protocole (paragraphe 3.b). Cela n'exclut pas que cette responsabilité soit engagée pour d'autres raisons que le fait d'avoir suivi l'injonction, comme un manquement à une quelconque obligation légale applicable selon laquelle un fournisseur de services doit assurer des conditions de sécurité suffisantes pour les données stockées. La forme de la mise en œuvre dépend des considérations juridiques et politiques des Parties; pour les Parties qui ont des exigences en matière de protection des données, il s'agirait notamment de définir une base claire pour le traitement des données à caractère personnel. Au vu des exigences supplémentaires prévues par les lois sur la protection des données pour autoriser d'éventuels transferts internationaux de données relatives aux abonnés, le présent Protocole traduit l'importance de l'intérêt public pour cette mesure de coopération directe et prévoit à son article 14 les garanties requises à cette fin.

101. Comme cela est énoncé ci-dessus, l'ordre juridique national d'une Partie détermine quelle autorité est considérée comme une autorité compétente pour adresser une injonction. Certaines Parties ont estimé de disposer d'une garantie supplémentaire permettant un contrôle plus poussé de la légalité de l'injonction (voir par exemple paragraphe 96 ci-dessus) en raison du caractère direct de la coopération. Alors que la Partie émettrice définit parmi ses autorités celles chargées d'adresser l'injonction, le paragraphe 2.b autorise les Parties à faire une déclaration selon laquelle « l'injonction adressée en application du paragraphe 1 doit être émise par un procureur ou une autre autorité judiciaire, sous la supervision de cette autorité ou sous une forme de supervision

indépendante ». Une Partie faisant usage de cette possibilité doit accepter toute injonction émise par l'une des autorités citées ou sous la supervision de l'une d'elles.

Paragraphe 3

102. Le paragraphe 3 de cet article précise les informations qui doivent, au minimum, être fournies par une autorité adressant une injonction en application du paragraphe 1 de cet article, bien qu'une Partie émettrice puisse décider d'inclure des renseignements complémentaires dans l'injonction elle-même pour faciliter son traitement ou parce que son droit interne lui impose de les y faire figurer. Les informations visées au paragraphe 3 sont particulièrement pertinentes pour l'exécution de l'injonction par le fournisseur de services, ainsi que pour l'intervention éventuelle de l'autorité de l'État partie dans lequel se trouve le fournisseur de services, conformément au paragraphe 5. L'injonction doit mentionner le nom de l'autorité émettrice et la date d'émission, donner des informations permettant d'identifier le fournisseur de services, préciser l'infraction qui fait l'objet de l'enquête ou de la procédure pénale, désigner l'autorité qui sollicite les données relatives aux abonnés et présenter une description détaillée des données spécifiques relatives aux abonnés qui sont demandées. L'injonction doit également contenir une déclaration selon laquelle elle est émise en application de ce Protocole; en faisant cette déclaration, la Partie indique que l'injonction est conforme aux dispositions du Protocole.

103. En ce qui concerne la différence entre le paragraphe 3.a (l'autorité émettrice) et le paragraphe 3.d. (l'autorité qui sollicite les données relatives aux abonnés), dans certaines Parties, l'autorité émettrice et l'autorité qui sollicite les données sont distinctes. Ainsi, les enquêteurs ou les procureurs peuvent jouer le rôle de l'autorité qui sollicite les données, alors que l'injonction est adressée par un juge. Dans de telles situations, il est alors nécessaire d'identifier l'autorité qui sollicite les données et celle qui émet l'injonction.

104. Il n'est pas nécessaire de produire un exposé des faits, étant donné que ces informations sont confidentielles dans la plupart des enquêtes pénales et qu'elles ne peuvent être divulguées à une partie privée.

Paragraphe 4

105. Alors que le paragraphe 3 énonce les informations qui doivent, au minimum, être transmises lors de l'émission d'une injonction au titre du paragraphe 1, ces injonctions ne peuvent souvent être exécutées que si le fournisseur de services (et, le cas échéant, l'autorité désignée par la Partie destinataire en application du paragraphe 5) reçoit des informations complémentaires. Par conséquent, le paragraphe 4 de cet article précise qu'une autorité émettrice doit fournir des informations complémentaires sur le fondement juridique interne qui habilite l'autorité à adresser une injonction; mentionner les dispositions juridiques et les sanctions applicables à l'infraction qui est à l'origine d'une enquête ou de poursuites; donner les coordonnées de l'autorité à laquelle le fournisseur de services doit communiquer les données relatives aux abonnés, demander de plus amples informations ou adresser toute autre réponse; indiquer le délai et le mode de communication de ces données; spécifier si une demande de conservation des données a été formulée précédemment, en précisant la date de conservation et tout numéro de référence applicable; évoquer tout type d'instructions spéciales en matière de procédure (demandes de confidentialité ou d'authentification) et ajouter toute autre information qui pourrait aider à obtenir la divulgation des données relatives aux abonnés. Il n'est pas nécessaire que les coordonnées fournies concernent précisément une personne, mais seulement une entité administrative. Ces renseignements complémentaires peuvent être transmis séparément mais peuvent également être inclus dans l'injonction elle-même, si la législation de la Partie émettrice le permet. L'injonction comme les informations complémentaires sont transmises directement au fournisseur de services.

106. Les instructions spéciales en matière de procédure portent notamment sur toute demande de confidentialité, y compris les demandes de non-divulgation de l'injonction à l'abonné concerné

ou à d'autres tiers. Si des mesures de confidentialité sont nécessaires pour éviter une divulgation prématurée de l'affaire, il faut l'indiquer dans la demande. Dans certains États parties, la confidentialité de l'injonction est maintenue de plein droit, alors que dans d'autres États parties ce n'est pas nécessairement le cas. Par conséquent, afin d'éviter tout risque de divulgation prématurée de l'enquête, les Parties sont encouragées à prendre connaissance de la législation applicable et des politiques des fournisseurs de services en matière de notification des abonnés, avant d'adresser l'injonction au fournisseur de services en application du paragraphe 1. En outre, au titre des instructions spéciales en matière de procédure, le moyen de transmission le plus adapté aux besoins de l'autorité peut être spécifié. Le fournisseur de services peut également demander des renseignements complémentaires concernant le compte ou d'autres informations pour l'aider à fournir une réponse rapide et complète. Une demande de confidentialité ne devrait pas empêcher les prestataires de services de rendre compte, dans un souci de transparence, des nombres agrégés anonymes d'ordres reçus au titre du présent article.

Paragraphe 5

107. Aux termes du paragraphe 5.a, une Partie peut notifier au Secrétaire Général du Conseil de l'Europe que, lorsqu'une commande est émise en vertu du paragraphe 1 à l'intention d'un prestataire de services sur son territoire, elle exigera une notification simultanée soit dans tous les cas (c'est-à-dire pour toutes les commandes transmises aux prestataires de services sur son territoire), soit dans des circonstances déterminées.

108. En application du paragraphe 5.b, une Partie peut également, en vertu de son droit interne, exiger d'un fournisseur de services qui se voit adresser une injonction par une autre Partie qu'il la consulte dans certaines circonstances déterminées. Une Partie ne peut pas exiger d'être consultée pour chaque injonction, car cela ajouterait une mesure supplémentaire qui pourrait retarder considérablement le traitement des demandes, mais seulement dans des circonstances limitées et définies. L'obligation de procéder à une consultation devrait être limitée aux circonstances dans lesquelles il y a un risque accru de devoir imposer des conditions ou invoquer un motif de refus ou une crainte de préjudice potentiel pour les enquêtes ou procédures pénales menées par la Partie transférante.

109. Les procédures de notification et de consultation sont laissées à l'entière discrétion des Parties, qui ne sont pas tenues d'exiger l'une ou l'autre.

110. Les Parties notifiées en vertu du paragraphe 5.a ou consultées en vertu du paragraphe 5.b peuvent ordonner à un fournisseur de services de ne pas divulguer des informations pour les motifs prévus au paragraphe 5.c, qui sont décrits plus en détail au paragraphe 141 du Rapport explicatif de l'article 8. De ce fait, la capacité d'une partie à être notifiée ou consultée constitue une garantie supplémentaire. Cela dit, la coopération doit en principe être étendue et les obstacles à celle-ci strictement limités. En conséquence, comme l'expliquent les paragraphes 242 et 253 du rapport explicatif de la convention, la détermination par la Partie notifiée ou consultée des conditions et des refus qui s'appliqueraient en vertu des articles 25, paragraphe 4, et 27, paragraphe 4, de la convention devrait également être limitée conformément aux objectifs de cet article, à savoir éliminer les obstacles à l'accès transfrontalier aux preuves électroniques aux fins d'enquêtes pénales et prévoir des procédures plus efficaces et accélérées dans ce domaine.

111. En vertu de paragraphe 5.d, les Parties qui font une déclaration en application du paragraphe 5.a ou qui exigent une consultation au titre du paragraphe 5.b peuvent contacter l'autorité désignée en vertu de l'article 4.c et lui demander des renseignements complémentaires pour déterminer s'il y a lieu, en vertu du paragraphe 5.c, d'ordonner au fournisseur de services de ne pas se conformer à l'injonction. Le processus se veut aussi rapide que les circonstances le permettent. La Partie notifiée ou consultée doit recueillir les informations nécessaires et prendre leur décision en vertu du paragraphe 5.c « dans les plus brefs délais ». Cette Partie doit également

informer rapidement les autorités de la Partie émettrice si elle décide d'ordonner au fournisseur de services de ne pas répondre favorablement, en indiquant les raisons de cette décision.

112. Une Partie qui exige d'être informée ou consultée peut décider d'imposer au fournisseur un délai d'attente avant qu'il ne fournisse les données relatives aux abonnés en réponse à l'injonction, afin de permettre la communication d'informations ou la tenue de la consultation et toute formulation de demandes de renseignements complémentaires par la Partie.

113. Aux termes du paragraphe 5.e, une Partie qui exige d'être informée ou consultée doit désigner une autorité unique et, lorsqu'une notification est requise en vertu du paragraphe 5.a, communiquer au Secrétaire Général du Conseil de l'Europe les coordonnées de cette autorité, et les Parties sont tenus de veiller à ce que les informations soient tenues à jour, y compris lorsque les Parties changent d'autorité unique désignées.

114. Une Partie peut modifier son exigence de notification ou de consultation à tout moment, selon les facteurs qu'elle juge pertinents, par exemple si elle souhaite passer d'un système de notification à un système de consultation ou si elle est suffisamment à l'aise avec la coopération directe pour pouvoir revoir ou annuler une obligation de notification ou de consultation adoptée précédemment. Elle peut également décider que, compte tenu de l'expérience qu'elle a acquise dans l'utilisation du mécanisme de coopération directe, elle souhaite instaurer un système de notification ou de consultation.

115. En vertu du paragraphe 5.f, le Secrétaire Général du Conseil de l'Europe est tenu d'établir et de tenir à jour un registre de toutes les exigences en matière de notification en vertu du paragraphe 5. La mise à disposition d'un registre public et à jour est essentielle pour garantir que les autorités de la Partie émettrice et les fournisseurs de services sont informés des exigences de notification de chaque Partie, lesquelles, comme indiqué ci-dessus, peuvent être modifiées à tout moment. Étant donné que toutes les Parties peuvent apporter une telle modification à leur discrétion, chaque Partie qui apporte une modification ou relève une inexactitude concernant ses données dans le registre est tenue d'en aviser immédiatement le Secrétaire Général afin de s'assurer que les autres Parties ont connaissance des exigences en vigueur et peuvent les appliquer correctement.

Paragraphe 6

116. Le paragraphe 6 indique clairement que la communication d'informations à une autre Partie et la fourniture d'informations supplémentaires par voie électronique, y compris par l'utilisation de courrier électronique et de portails électroniques, est autorisée. Si le fournisseur de services le juge acceptable, une Partie peut soumettre une commande en vertu du paragraphe 1 et des informations supplémentaires en vertu du paragraphe 4 sous forme électronique. L'objectif est d'encourager le recours à des moyens électroniques s'ils sont acceptables pour le prestataire de services, car ce sont presque toujours les moyens de communication les plus efficaces et les plus rapides. Les méthodes d'authentification appliquées peuvent comprendre divers moyens, utilisés éventuellement en les associant, pour permettre une identification sécurisée de l'autorité requérante. Ces moyens peuvent par exemple être les suivants: l'obtention d'une confirmation d'authenticité par l'intermédiaire d'une autorité connue au sein de la Partie émettrice (auprès de l'expéditeur ou d'une autorité centrale ou désignée, par exemple); des communications ultérieures entre l'autorité émettrice et la Partie destinataire; l'utilisation d'une adresse électronique officielle ou de futures méthodes de vérification technologique qui peuvent être facilement utilisées par les autorités qui transmettent les informations. Des dispositions similaires figurent au paragraphe 2 de l'article 10 et d'autres orientations concernant les exigences en matière de sécurité sont proposées au paragraphe 175 du Rapport explicatif. L'article 6, paragraphe 4, et l'article 8 contient également des dispositions similaires, au paragraphe 5.

Paragraphe 7

117. Le paragraphe 7 prévoit que, si un fournisseur de services ne se conforme pas à l'injonction adressée au titre de cet article, la Partie émettrice ne peut en demander l'exécution qu'en application de l'article 8 ou d'une autre forme d'entraide. Les Parties qui invoquent cet article ne peuvent chercher à obtenir une exécution unilatérale.

118. S'agissant de l'exécution de l'injonction au moyen de l'article 8, le Protocole envisage une procédure simplifiée de conversion d'une injonction émise en vertu de cet article en une injonction émise en application de l'article 8 afin qu'il soit plus facile, pour la Partie émettrice, d'obtenir des données relatives aux abonnés.

119. Afin d'éviter les doublons, une Partie émettrice doit accorder au fournisseur de services un délai de 30 jours ou le délai prévu au sous-paragraphe 4.d, la plus longue période étant retenue, pour que le processus de notification et de consultation ait lieu et que le fournisseur de services communique les informations demandées ou indique son refus de le faire. Ce n'est qu'après l'expiration de ce délai, ou si le fournisseur a indiqué son refus de se conformer à l'injonction avant l'expiration de ce délai, qu'une Partie émettrice peut demander son exécution au titre de l'article 8 ou d'autres formes d'entraide. Pour permettre aux autorités d'évaluer s'il y a lieu de demander l'exécution en vertu du paragraphe 7, les fournisseurs de services sont encouragés à donner les raisons pour lesquelles ils n'ont pas transmis les données demandées. Un fournisseur de services peut par exemple expliquer que ces données ne sont plus disponibles.

120. Si une autorité informée en application du paragraphe 5.a ou consultée au titre du paragraphe 5.b a informé la Partie émettrice que le fournisseur de services a reçu instruction de ne pas divulguer les informations demandées, la Partie émettrice peut néanmoins demander l'exécution de son injonction au moyen de l'article 8 ou d'une autre forme d'entraide. Toutefois, il existe un risque de rejet de cette nouvelle demande. Il est conseillé à la Partie émettrice de consulter à l'avance une autorité désignée en application des paragraphes 5.a ou 5.b afin de remédier à toute insuffisance de l'injonction initiale et d'éviter de transmettre des injonctions au moyen de l'article 8 ou de tout autre mécanisme d'entraide qui pourrait donner lieu à un refus.

Paragraphe 8

121. Aux termes du paragraphe 8, une Partie peut déclarer qu'une autre Partie doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en application de l'article 8, à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait. Ainsi, une Partie peut faire une telle déclaration parce qu'elle considère que les procédures prévues par cet article devraient permettre aux autres Parties d'obtenir des données relatives aux abonnés plus rapidement qu'en invoquant l'article 8 et, par conséquent, pourraient réduire le nombre de cas dans lesquels l'article 8 doit être invoqué. Les procédures prévues par l'article 8 ne seraient alors utilisées que lorsque les démarches visant à obtenir la divulgation de données relatives aux abonnés directement auprès du fournisseur de services ont échoué, lorsque la Partie émettrice a une explication raisonnable pour ne pas appliquer cet article en premier lieu ou lorsque la Partie émettrice s'est réservé le droit de ne pas appliquer cet article. Une Partie émettrice peut ainsi en faire la démonstration lorsqu'un fournisseur de services s'abstient régulièrement de transmettre des données relatives aux abonnés en réponse à des injonctions adressées directement par cette Partie. Autre exemple, si une Partie émettrice, au moyen d'une injonction unique, demande la divulgation de données relatives aux abonnés et de données relatives au trafic à une autre Partie qui applique l'article 8 à ces deux catégories de données, la Partie émettrice n'a pas besoin de demander dans un premier temps les données relatives aux abonnés séparément.

Paragraphe 9

122. En vertu du paragraphe 9.a, une Partie qui se réserve le droit de ne pas appliquer cet article n'est pas tenue de prendre des mesures en application du paragraphe 2 pour que les fournisseurs de services sur son territoire divulguent des données relatives aux abonnés en réponse à des injonctions adressées par d'autres Parties. Une Partie qui se réserve ce droit n'est pas autorisée à adresser des injonctions au titre du paragraphe 1 à des fournisseurs de services sur le territoire d'autres Parties.

123. Le paragraphe 9.b dispose que – pour les raisons mentionnées au paragraphe 92 ci-dessus – si la divulgation de certains types de numéros d'accès en vertu de cet article serait incompatible avec les principes fondamentaux de son ordre juridique interne, une Partie peut se réserver le droit de ne pas appliquer cet article à ces numéros. Une Partie qui formule une telle réserve n'est pas autorisée à adresser des injonctions concernant ces numéros au titre du paragraphe 1 à des fournisseurs de services sur le territoire d'autres Parties.

Section 3 – Procédures complétant la coopération internationale et l'entraide existantes entre les autorités

Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données

124. Cet article a pour but de donner à une Partie requérante la capacité d'émettre une injonction à produire à une Partie requise, dans le cadre d'une demande, et de faire en sorte que la Partie requise soit en mesure de donner effet à ladite injonction en ordonnant à un fournisseur de services sur son territoire de produire des informations sur l'abonné ou des données relatives au trafic qui sont en possession ou sous le contrôle du fournisseur de services.

125. Cet article établit un mécanisme qui complète les dispositions de la Convention relatives à l'entraide judiciaire. Il est conçu pour être plus simple que l'entraide judiciaire actuelle, puisque les informations que doit fournir la Partie requérante sont plus limitées et le processus d'obtention des donnés plus rapide. Il complète sans pour autant remplacer d'autres processus d'entraide judiciaire prévus par la Convention, ou d'autres accords multilatéraux ou bilatéraux, qu'une Partie demeure libre d'invoquer. De fait, lorsqu'une Partie requérante souhaite demander des données relatives au trafic à une Partie qui a émis une réserve concernant cet aspect de cet article, la Partie requérante peut recourir à une autre procédure d'entraide judiciaire. Lorsque, comme c'est fréquemment le cas, la demande porte sur la production simultanée d'informations sur l'abonné, de données relatives au trafic et de données relatives au contenu stocké, il peut être plus efficient de demander les trois formes de données à partir du même compte au moyen d'une seule demande d'entraide traditionnelle plutôt que de demander certains types de données au moyen de la méthode prévue par cet article pour d'autres types de données au moyen d'une demande d'entraide distincte.

Paragraphe 1

126. Le paragraphe 1 dispose que la Partie requérante doit être en mesure d'émettre une injonction en vue d'obtenir des informations relatives à l'abonné ou données relatives au trafic détenues par un fournisseur de services sur le territoire d'une autre Partie. Le terme « injonction » utilisé dans le présent article signifie tout processus judiciaire ayant pour but d'obliger un fournisseur de services à fournir des informations relatives à un abonné ou données relatives au trafic. L'injonction peut ainsi prendre la forme d'une injonction de produire, d'une assignation ou autre mécanisme autorisé en droit et qui peut être émis pour ordonner la production d'informations relatives à un abonné ou données relatives au trafic.

127. Tel que cela est défini au paragraphe 2.b de l'Article 3, l'expression « autorité compétente » au paragraphe 1 du présent article recouvre « une autorité judiciaire, administrative ou répressive

compétente en droit interne pour ordonner, autoriser ou entreprendre l'exécution de mesures en vertu de ce Protocole en vue de la collecte ou de la production de preuves concernant des enquêtes criminelles ou procédures pénales spécifiques ». On relèvera que les autorités compétentes pour émettre une injonction en vertu du paragraphe 1 ne seront pas nécessairement les mêmes que les autorités désignées pour soumettre l'injonction à laquelle il convient de donner effet conformément au paragraphe 10 a) du présent article, comme décrit de manière plus détaillée ci-dessous.

128. Dans cet article, l'expression « un fournisseur de services sur le territoire d'une autre Partie » requiert que le fournisseur de services soit physiquement présent sur le territoire de l'autre Partie. En vertu de cet article, le simple fait que, par exemple, un fournisseur de services ait établi une relation contractuelle avec une société dans une Partie, mais qu'il ne soit pas lui-même physiquement présent dans cette Partie ne le qualifierait comme étant « sur le territoire » de cette Partie. Le paragraphe 1 requiert en outre que les données soient en possession ou sous le contrôle du fournisseur de services.

Paragraphe 2

129. En vertu du paragraphe 2, la Partie requise adopte les mesures nécessaires aux fins de donner effet sur son territoire à une injonction émise en vertu du paragraphe 1, sous réserve des garanties qui vont être décrites ci-après. « Donner effet » signifie que la Partie requise devra ordonner au fournisseur de services de communiquer les informations relatives à l'abonné et données relatives au trafic en utilisant le mécanisme correspondant au choix de la Partie requise, à condition que le mécanisme rende l'injonction exécutoire dans le droit interne de la Partie requise et respecte les dispositions du présent article. Par exemple, une Partie requise peut donner effet à l'injonction émanant d'une Partie requérante en acceptant l'injonction comme équivalente à des injonctions émises dans son droit interne, en l'endossant pour lui donner la même force exécutoire qu'une injonction émise dans son droit interne ou en émettant sa propre injonction de production. Quel que soit le mécanisme choisi, il sera soumis aux dispositions du droit interne de la Partie requise, puisque ce sont les procédures de cette dernière qui l'encadreront. La Partie requise peut ainsi s'assurer que son propre droit, y compris les conditions en matière constitutionnelle et de droits de l'homme, est respecté tout particulièrement pour ce qui est des éventuelles garanties supplémentaires, y compris celles qui sont nécessaires en matière de production des données relatives au trafic.

130. Il existe certes diverses manières d'appliquer cet article, et une Partie peut souhaiter concevoir ses propres processus internes en y intégrant la flexibilité nécessaire pour traiter les demandes émanant de toute une série d'autorités compétentes diverses et variées. Le paragraphe 3.b a été négocié pour garantir que la Partie requise se voie fournir suffisamment d'informations pour qu'un examen complet puisse être mené au besoin, car certaines Parties ont indiqué qu'elles émettraient leurs propres injonctions pour donner effet à celle de la Partie requise.

Paragraphe 3

131. Pour déclencher auprès de la Partie requise le processus qui donnera effet à l'injonction, la Partie requérante transmet l'injonction et les informations à l'appui de cette dernière. Le paragraphe 3 décrit ce qu'une Partie requérante doit communiquer à la Partie requise pour que celle-ci donne effet à l'injonction et enjoigne à un prestataire de service sur son territoire de produire les éléments demandés. L'alinéa 3.a décrit les informations devant figurer dans l'injonction elle-même et inclut des informations fondamentales pour l'exécution de l'injonction. Les informations visées par le paragraphe 3.b, uniquement à l'usage de la Partie requise et qui ne doivent pas être communiquées avec le fournisseur de services sauf sur autorisation de la Partie requérante, sont des informations en appui à l'injonction qui posent dans le présent Protocole la base juridique nationale et internationale pour l'injonction, et sert à la Partie requise pour évaluer les motifs potentiels d'une réponse conditionnelle ou d'un refus en vertu du paragraphe 8. Lorsqu'elles envoient une demande en vertu de cet article, les Parties devraient indiquer si des informations relevant du paragraphe 3.b

peuvent être partagées avec le fournisseur de services. En vertu du paragraphe 3.c, la demande devrait aussi au moment de sa transmission et afin de garantir le traitement correct de la demande, inclure toutes instructions spéciales, par exemple des demandes pour une certification ou de confidentialité de la demande (similairement à l'article 27, paragraphe 8, de la Convention).

132. L'injonction de produire des informations concernant l'abonné ou de données concernant le trafic décrite au paragraphe 3.a. doit, sur sa première page, mentionner le nom du ou des fournisseurs de services devant être notifiés, la mention que l'injonction est émise conformément au présent Protocole, une description détaillée des données spécifiques demandées (autrement dit l'identité de l'abonné, l'adresse postale ou géographique, le numéro de téléphone ou autre numéro d'accès ainsi que les informations relatives à la facturation et au règlement disponibles du fait du contrat ou des modalités de service (voir l'article 3 du présent Protocole incorporant l'article 18, paragraphe 3, de la Convention et du Rapport explicatif paragraphe 93 ci-dessus); et pour ce qui est des données relatives au trafic, les données informatiques concernant une communication au moyen d'un système informatique, générées par un système informatique qui faisait partie de la chaîne de communication indiquant l'origine, la destination, le routage, l'heure, la date, la durée ou le type de services sous-jacent (voir l'article 3, paragraphe 1 de ce Protocole incorporant l'article 1, paragraphe d, de la Convention), l'autorité qui a émis l'injonction, l'autorité qui demande les données, et l'infraction qui fait l'objet de l'enquête criminelle ou de la procédure pénale. Si l'autorité émettrice et celle qui demande les données sont différentes, en vertu de la disposition, les deux doivent être identifiées. Ainsi, une autorité d'enquête ou de poursuite peut être celle qui demande les données et un juge celui qui émet l'injonction. Ces informations viennent à l'appui de la légitimité de l'injonction et de la clarté des instructions pour son exécution.

133. Les informations en appui décrites à l'alinéa 3.b. ont pour but de communiquer à la Partie requise les informations dont elle a besoin pour donner effet à l'injonction de la Partie requérante. Il serait également possible de faciliter leur communication en recourant à un formulaire facile à remplir qui rendrait le processus encore plus efficient et recueillerait notamment les éléments suivants:

a. au titre de l'alinéa 3.b.i, la base légale qui donne compétence à l'autorité émettrice pour émettre l'injonction visant à obliger le fournisseur de services à produire les données demandées. En d'autres termes, cette rubrique comprendra la loi pertinente qui donne pouvoir à une autorité compétente pour émettre l'injonction décrite au paragraphe 1;

b. au titre de l'alinéa 3.b.ii, la disposition juridique concernant l'infraction mentionnée dans l'injonction telle que visée à l'alinéa 3.a.iv et le barème de sanctions qui lui est associé. L'inclusion de ces deux éléments est important pour que la Partie requise évalue si la demande entre dans le périmètre de ses obligations;

c. au titre de l'alinéa 3.b.iii, toutes informations pouvant être fournies par la Partie requérante qui l'ont amenée à conclure que le ou les fournisseurs de services visés par l'injonction sont en possession des informations ou données demandées ou en ont le contrôle. Ces informations sont fondamentales pour démarrer le processus dans la Partie requise. L'identification du fournisseur national de services et le fait de penser que celui-ci possède ou contrôle les informations ou données requises est souvent une condition préalable à l'émission d'une demande d'injonction de produire;

d. au titre de l'alinéa 3.b.iv, un bref résumé des faits liés à l'enquête ou à la procédure. Ces informations sont également essentielles pour que la Partie requise détermine s'il convient ou non de donner effet à une injonction sur son territoire;

e. au titre de l'alinéa 3.b.v, une déclaration concernant la pertinence des informations ou données pour l'enquête ou la procédure. Cette déclaration est destinée à aider la Partie requise à décider si les conditions prévues au paragraphe 1 de cet article sont remplies, autrement dit si les informations ou données sont « nécessaires pour les enquêtes ou procédures pénales spécifiques de la Partie requérante »;

f. au titre de l'alinéa 3.b.vi, les coordonnées de contact d'une ou de plusieurs autorités si l'autorité compétente dans la Partie requise a besoin d'informations supplémentaires pour donner effet à l'injonction;

g. au titre de l'alinéa 3.b.vii, des précisions concernant l'éventualité que la conservation des informations ou données a déjà été demandée. Cette information est importante pour la Partie requise, en particulier pour ce qui concerne les données liées au trafic, et devrait préciser, par exemple, les références de la demande et la date de la conservation, car elle permet à la Partie requise de rapprocher la demande nouvellement reçue d'une demande antérieure de conservation, et ainsi de faciliter la communication des informations ou données conservées à l'origine. Pour réduire le risque que des informations ou données soient effacées, les Parties sont encouragées à demander au plus tôt la conservation des informations ou données recherchées et de le faire avant d'intenter une demande d'entraide en vertu du présent article, ainsi que de veiller à ce que l'extension de la préservation soit demandée en temps opportun;

h. au titre de l'alinéa 3.b.iii, des précisions sur l'éventualité que les données aient déjà été demandées par d'autres moyens et si oui, comment. Cette disposition concerne essentiellement le cas où une Partie requérante a déjà sollicité directement auprès du fournisseur de service des informations relatives à l'abonné ou des données relatives au trafic.

134. Les informations à fournir en vertu de l'alinéa 3.b ne sont pas communiquées au fournisseur de services sans l'accord de la Partie requérante. En particulier, le résumé des faits et la déclaration concernant la pertinence des informations ou données pour l'enquête ou les poursuites est communiqué à la Partie requise pour déterminer s'il y a lieu d'imposer des termes ou conditions ou de refuser, mais relève souvent du secret de l'enquête.

135. En vertu de l'alinéa 3.c, la Partie requérante peut demander des instructions procédurales spécifiques, dont des demandes de non-divulgation de l'injonction à l'abonné ou des formulaires d'authentification à remplir pour la preuve. Ces informations doivent être connues dès le départ, étant donné que certaines instructions spéciales peuvent entraîner des processus supplémentaires chez la Partie requise.

136. Pour donner effet à l'injonction et faciliter davantage la production des informations et données, la Partie requise peut communiquer au fournisseur de services des informations complémentaires telles que la méthode de production, et le destinataire de la production des données chez la Partie requise.

Paragraphe 4

137. En vertu du paragraphe 4, il peut être nécessaire de fournir des informations complémentaires à la Partie requise pour donner effet à l'injonction. Ainsi, dans les lois nationales de certaines Parties, la production de données sur le trafic peut exiger la communication d'informations supplémentaires du fait de conditions supplémentaires dans ce droit pour l'obtention de ces données. De plus, la Partie requise peut demander des éclaircissements concernant les informations fournies en vertu de l'alinéa 3.b. ou encore des Parties peuvent demander des informations supplémentaires lorsque l'injonction n'a pas été émise ou revue par un procureur ou une autre autorité administrative judiciaire ou indépendante de la Partie requérante. Les Parties qui feront ce type de déclaration devraient être aussi spécifiques que possible pour ce qui concerne le type d'informations complémentaires requises.

Paragraphe 5

138. Le paragraphe 5 exige que la Partie requise accepte les demandes sous forme électronique. Il peut exiger l'utilisation de moyens de communication électroniques sûrs et authentifiables pour faciliter la transmission d'informations ou de données et de documents, y compris la transmission

d'ordonnances et de renseignements à l'appui. Les articles 6 à 11 prévoient également de tels moyens de communication.

Paragraphe 6

139. En vertu du paragraphe 6, la Partie requise devrait prendre des mesures pour traiter rapidement la demande. Elle fait des efforts raisonnables pour traiter les demandes et notifier le fournisseur de services dans les 45 jours suivant sa réception de tous les documents et informations nécessaires. La Partie requise ordonnera au fournisseur de services de produire les informations relatives à l'abonné dans les 20 jours et les données relatives au trafic dans les 45 jours. La Partie reuise devrait certes s'efforcer d'obtenir la production aussi rapidement que possible, toutefois de nombreux facteurs peuvent retarder celle-ci, par exemple les objections des fournisseurs de services, le fait que ces derniers ne répondent pas aux demandes ou ne respectent pas les délais pour la production, mais aussi le volume de demandes qu'une Partie requise peut se voir demander de traiter. Il a donc été décidé d'exiger que les Parties requises fassent des efforts raisonnables pour mener à bien uniquement les processus sous leur contrôle.

Paragraphe 7

140. Les Parties ont reconnu que certaines instructions procédurales spéciales demandées par la Partie requérante peuvent aussi causer des retards dans le traitement des injonctions, si les instructions requièrent des processus nationaux supplémentaires pour donner effet aux instructions procédurales spéciales. La Partie requise peut aussi demander des informations supplémentaires à la Partie requérante pour étayer toutes demandes d'injonctions supplémentaires telles que des injonctions de confidentialité (injonctions de non-divulgation). Certaines instructions procédurales peuvent ne pas être prévues dans le droit de la Partie requise, auquel cas le paragraphe 7 prévoit que celle-ci en informe rapidement la Partie requérante et spécifie les conditions dans lesquelles elle pourrait donner suite à la demande, ce qui permet alors à la Partie requérante de déterminer si elle souhaite ou non poursuivre avec sa demande.

Paragraphe 8

141. En vertu du paragraphe 8, la Partie requise peut refuser d'exécuter une requête si les motifs de refus établis aux articles 25, paragraphe 4 ou 27, paragraphe 4 de la Convention existent. Par exemple, conformément au paragraphe 257 du Rapport explicatif de la Convention, cette disposition est soumise aux motifs de refus prévus par les traités d'entraide judiciaire et les lois nationales applicables et offre "des garanties pour les droits des personnes se trouvant dans la Partie requise", et conformément au paragraphe 268 de ce même Rapport explicatif, l'entraide peut être refusée pour "atteinte à la souveraineté de l'État, à la sécurité, à l'ordre public ou à d'autres intérêts essentiels". Elle peut également imposer les conditions nécessaires pour permettre l'exécution de la demande, telles que la confidentialité. En outre, la Partie requise peut différer l'exécution de la requête en vertu de l'article 27, paragraphe 5, de la Convention. La Partie requise notifie à la Partie requérante sa décision de refuser, de conditionner ou de différer la demande. En outre, les Parties peuvent appliquer une limitation de l'usage conformément aux termes de l'article 28, paragraphe 2.b de la Convention.

142. Afin de promouvoir le principe de la coopération la plus large possible (voir article 5, paragraphe 1), les motifs de refus établis par une Partie requise devraient être étroits et exercés avec retenue. Il convient de rappeler que le paragraphe 253 du Rapport explicatif de la Convention prévoit que « l'entraide doit en principe être étendue et les entraves dont elle peut faire l'objet doivent être strictement limitées. » En conséquence, les conditions et refus devraient également être limités conformément aux objectifs de cet article pour éliminer les obstacles au partage transfrontalier des informations relatives à l'abonné et des données relatives au trafic et pour mettre en place des procédures plus efficientes et rapides que l'entraide traditionnelle.

Paragraphe 9

143. En vertu du paragraphe 9, « si une Partie requérante ne peut se conformer à une condition imposée par la Partie requise en vertu du paragraphe 8, elle en informe rapidement la Partie requise. La Partie requise détermine alors si les informations ou le matériel doivent néanmoins être fournis. Si la Partie requérante accepte la condition, elle est liée par celle-ci. La partie requise qui fournit des renseignements ou du matériel soumis à une telle condition peut exiger de la partie requérante qu'elle explique, en relation avec cette condition, l'usage qui a été fait de ces renseignements ou de ce matériel ».

Paragraphe 10

144. L'objet du paragraphe 10 est de faire en sorte que les Parties, au moment de la signature, ou au moment du dépôt de leurs instruments de ratification, d'acceptation ou d'approbation, identifient les autorités chargées de soumettre et de recevoir les commandes en vertu du présent article. Les Parties ne sont pas tenues de donner le nom et l'adresse d'une personne en particulier, mais peuvent identifier un bureau ou une unité qui a été jugé compétent aux fins de l'envoi et de la réception des ordres en vertu du présent article.

Paragraphe 11

145. Le paragraphe 11 permet à une Partie de déclarer qu'elle demande que les injonctions qui lui sont soumises en vertu de cet article soient transmises par l'autorité centrale de la Partie requérante ou une autre autorité s'il en est ainsi convenu ensemble par les Parties. Les Parties sont encouragées à prévoir la plus grande souplesse pour la soumission de demandes.

Paragraphe 12

146. Le paragraphe 12 requiert que le Secrétaire Général ou la Secrétaire Générale du Conseil de l'Europe établisse et tienne à jour un registre des autorités désignées par les Parties en vertu du paragraphe 10 et que chaque Partie veille à ce que ses informations contenues dans le registre soient justes et précises. Ces informations aideront les Parties requises à vérifier l'authenticité des demandes.

Paragraphe 13

147. En vertu du paragraphe 13, une Partie qui se réserve le droit de ne pas appliquer cet article aux données relatives au trafic n'est pas tenue de donner effet à des injonctions de production de données relatives au trafic émanant d'une autre Partie. Une Partie qui émet des réserves concernant cet article n'est pas autorisée à soumettre des injonctions de production de données relatives au trafic à d'autres Parties en vertu du paragraphe 1.

Article 9 – Divulgation rapide de données informatiques stockées en cas d'urgence

148. Outre les autres formes de coopération accélérée prévues par le Protocole, les rédacteurs étaient conscients de la nécessité de faciliter la capacité des Parties d'obtenir rapidement, dans une situation d'urgence spécifiée, des données informatiques stockées en possession ou sous le contrôle d'un fournisseur de services sur le territoire d'une autre Partie pour les utiliser dans le cadre d'enquêtes ou de procédures pénales spécifiques. Comme indiqué dans les paragraphes 42 et 172 du Rapport explicatif, il peut être nécessaire de demander une coopération la plus rapide possible dans diverses situations où l'urgence est un facteur primordial, juste après une attaque terroriste par exemple, après une attaque par rançongiciel qui peut paralyser le système d'un hôpital, ou lors de l'enquête sur les comptes de messagerie utilisés par les ravisseurs pour faire connaître des exigences et communiquer avec la famille de la victime.

149. En vertu de la Convention, dans des situations d'urgence, les Parties font des demandes d'entraide pour obtenir des données et, en vertu de l'article 35, paragraphe 1.c, de la Convention, le Réseau 24/7 est disponible pour faciliter l'exécution de ces demandes. En outre, les systèmes juridiques de quelques pays permettent aux autorités compétentes d'autres pays de demander la divulgation d'urgence des données par l'intermédiaire du Réseau 24/7 sans envoyer de demande d'entraide.

150. Comme indiqué dans l'article 5, paragraphe 7, ce présent article ne porte pas atteinte à la coopération (y compris spontanée) entre les Parties ou entre les Parties et les fournisseurs de services par le biais d'autres accords, arrangements, pratiques ou lois nationales applicables. Par conséquent, en vertu du Protocole, tous les mécanismes susmentionnés restent à la disposition des autorités compétentes qui demandent des données en situation urgente. L'innovation du Protocole est l'élaboration de deux articles qui obligent toutes les Parties à fournir, au minimum, des voies spécifiques pour une coopération accélérée pouvant être activée rapidement dans les situations urgentes, à savoir le présent article et l'article 10.

151. Le présent article permet aux Parties de coopérer pour obtenir des données informatiques dans des situations d'urgence en utilisant comme canal le Réseau 24/7 établi par l'article 35 de la Convention. Le Réseau 24/7 est particulièrement bien adapté pour traiter les demandes pour lesquelles le facteur temps est crucial et hautement prioritaires prévues au présent article. Le Réseau est doté de Points de Contact qui, dans la pratique, communiquent rapidement et sans avoir besoin de traductions écrites et sont en mesure d'exécuter les demandes reçues d'autres Parties, que ce soit en allant directement auprès de fournisseurs sur leur territoire, en sollicitant l'aide d'autres autorités compétentes ou en s'adressant aux autorités judiciaires, si cette condition est prévue par la loi nationale de la Partie. Ces Points de Contact peuvent également conseiller les Parties requérantes sur des questions qu'elles pourraient se poser concernant les fournisseurs et la collecte de preuves électroniques, par exemple, en expliquant le cadre de la loi nationale qui doit être satisfait pour obtenir des éléments de preuve. Cette communication en aller-retour améliore la compréhension par la Partie requérante du droit interne dans la Partie requise et permet un recueil plus facile des éléments de preuve nécessaires.

152. L'utilisation du canal prévu au présent article peut avoir des avantages par rapport au canal d'entraide judiciaire d'urgence énoncé à l'article10. Par exemple, ce canal présente l'avantage de ne pas nécessiter la préparation à l'avance d'une demande d'entraide. Il faut parfois beaucoup de temps pour préparer au préalable une demande d'entraide, la faire traduire et la transmettre par les voies nationales à l'autorité centrale de la Partie requérante compétente en matière d'entraide, ce qui ne serait pas nécessaire en vertu du présent article. En outre, une fois que la Partie requise a reçu la demande, si elle doit obtenir des renseignements supplémentaires avant de pouvoir accorder une aide, le temps supplémentaire qui peut être nécessaire pour une demande d'entraide est susceptible de ralentir l'exécution de la demande. Dans le contexte de l'entraide, les Parties requises exigent souvent que les informations supplémentaires soient fournies sous une forme écrite et plus détaillée, alors que le canal 24/7 fonctionne par l'échange d'informations en temps réel. D'autre part, le canal de l'entraide judiciaire urgente offre des avantages dans certaines situations. Par exemple, (1) on ne perd pas ou peu de temps en utilisant ce canal s'il existe des relations de travail particulièrement étroites entre les autorités centrales concernées; (2) l'entraide d'urgence peut être utilisée pour obtenir des formes supplémentaires de coopération au-delà des données informatiques détenues par les fournisseurs, et (3) il peut être plus facile d'authentifier les éléments de preuve obtenus par l'intermédiaire de l'entraide judiciaire. Il appartient aux Parties, sur la base de leur expérience et des circonstances juridiques et factuelles spécifiques en cause, de décider quel est le meilleur canal à utiliser dans un cas particulier.

Paragraphe 1

153. En vertu du paragraphe 1.a, chaque Partie adopte les mesures nécessaires pour s'assurer que son Point de Contact pour le Réseau 24/7 est en mesure de transmettre les demandes en cas d'urgence au Point de Contact d'une autre Partie demandant une assistance immédiate pour obtenir la divulgation accélérée des données informatiques spécifiées et stockées détenues par les fournisseurs sur le territoire de cette Partie et recevoir des demandes de Points de Contact dans d'autres Parties concernant lesdites données détenues par des fournisseurs sur son territoire. Comme le prévoit l'Article 2, la demande doit être présentée dans le cadre d'une enquête ou procédure pénale spécifique.

154. Les Points de Contact 24/7 doivent avoir la capacité de transmettre et de recevoir ces demandes en cas d'urgence sans qu'une demande d'entraide doive être préparée et transmise à l'avance comme décrit au paragraphe 152 du Rapport explicatif ci-dessus, sous réserve de la possibilité d'une déclaration au titre de l'article 9, paragraphe 5. Le terme « urgente » est défini à l'article 3. En vertu du présent article, la Partie requise devra déterminer s'il existe une « urgence » par rapport à une demande en utilisant les informations fournies au paragraphe 3.

155. Contrairement à d'autres articles du présent Protocole, tels que l'Article 7, qui ne peuvent être utilisés que pour obtenir des « informations relatives à l'abonné spécifiées et stockées », le présent article utilise l'expression plus large « données informatiques spécifiées et stockées ». Le champ d'application de cette expression est large mais il n'est pas générique: il couvre les données informatiques « spécifiées » telles que définies à l'article 1.b de la Convention, qui est repris à l'article 3, paragraphe 1, du présent Protocole.. L'utilisation de cette expression plus large reconnaît l'importance d'obtenir du contenu stocké et des données de trafic, et pas uniquement des informations relatives à l'abonné, dans des situations d'urgence sans exiger la présentation d'une demande d'entraide comme condition préalable. Les données en question sont stockées ou existantes et n'incluent pas de données qui n'existent pas encore, telles que les données de trafic ou les données de contenu relatives aux communications futures (voir le Rapport explicatif de la Convention, paragraphe 170.)

156. Cette disposition offre à la Partie requérante la latitude nécessaire pour déterminer quelles autorités devraient la présenter, par exemple ses autorités compétentes qui mènent l'enquête, ou son Point de Contact 24/7, conformément au droit interne. Le Point de Contact du Réseau 24/7 de la Partie requérante fonctionne alors comme canal pour transmettre la demande au Point de Contact 24/7 de l'autre Partie.

157. En vertu du paragraphe 1.b, une Partie peut déclarer qu'elle n'exécutera pas une demande en vertu du présent article visant uniquement des informations relatives à l'abonné, telles que définies à l'article 18.3 de la Convention, incorporées à l'article 3, paragraphe 1, du présent Protocole. Pour certaines Parties, recevoir des demandes en vertu du présent article uniquement pour des informations relatives aux abonnés risquerait de surcharger les Points de Contact du Réseau 24h/7 en détournant les ressources et l'énergie des demandes de contenu ou de données relatives au trafic. Dans de tels cas, les Parties qui ne cherchent qu'à obtenir des informations sur les abonnés peuvent plutôt utiliser les articles 7 ou 8, qui facilitent la divulgation rapide de ces informations. Une telle déclaration n'interdit pas à d'autres Parties d'inclure une demande d'informations relatives aux abonnés lorsqu'elles émettent également une demande en vertu du présent article pour le contenu et/ou les données relatives au trafic.

Paragraphe 2

158. Le paragraphe 2 exige que chaque Partie adopte les mesures nécessaires pour que ses autorités soient habilitées, en vertu de sa loi nationale, à demander et à obtenir des données demandées en vertu du paragraphe 1 auprès des fournisseurs de services sur son territoire et à

répondre à ces demandes sans que la Partie requérante n'ait à présenter une demande d'entraide, sous réserve de pouvoir faire une déclaration conformément au paragraphe 5.

159. Compte tenu des différences entre droits internes, le paragraphe 2 vise à donner aux Parties la souplesse nécessaire pour la construction de leurs systèmes de réponse aux demandes en vertu du paragraphe 1. Les Parties sont toutefois encouragées à élaborer des mécanismes conformes au présent article qui mettent l'accent sur la rapidité et l'efficacité, sont adaptés aux exigences d'une situation d'urgence et donnent une base juridique générale pour la divulgation aux autres Parties de données dans les situations d'urgence.

160. Il appartient à la Partie requise de déterminer: (1) si les conditions permettant d'invoquer le présent article ont été remplies; 2) si un autre mécanisme est approprié pour aider la Partie requérante; (3) l'autorité compétente pour exécuter une demande reçue par le Point de Contact du Réseau 24/7. Bien que le Point de Contact du Réseau 24/7 de certaines Parties puisse déjà avoir la compétence requise pour exécuter la demande lui-même, d'autres Parties peuvent exiger que le Point de Contact transmette la demande à une ou d'autres autorités pour demander au fournisseur de divulguer les données. Dans certaines Parties, cela peut dépendre de l'obtention d'une ordonnance judiciaire pour demander la divulgation des données. La Partie requise a également tout pouvoir pour déterminer le canal à utiliser pour transmettre les données en réponse à la Partie requérante, que ce soit par l'intermédiaire du Point de Contact 24/7 ou par l'intermédiaire d'une autre autorité.

Paragraphe 3

161. Le paragraphe 3 précise les informations à fournir dans une demande formulée en vertu du paragraphe 1. Les informations spécifiées au paragraphe 3 visent à faciliter l'examen et, le cas échéant, l'exécution de la demande par l'autorité compétente de la Partie requise.

162. En ce qui concerne le paragraphe 3.a, la Partie requérante précise l'autorité compétente au nom de laquelle les données sont demandées.

163. En ce qui concerne le paragraphe 3.b, la Partie requérante doit indiquer que la demande est émise conformément au présent Protocole. Cela permettra d'assurer que la demande est faite conformément au Protocole et que toutes les données reçues en conséquence seront traitées d'une manière conforme aux exigences du Protocole. Cela permettra également de différencier la demande des autres demandes de divulgation d'urgence que le Point de Contact du Réseau 24/7 pourrait recevoir.

164. En application du paragraphe 3.e, la Partie requérante doit communiquer suffisamment de faits à l'appui de l'existence d'une situation urgente, telle que définie à l'article 3, et expliquer comment les données recherchées par la demande se rapportent à ladite situation. Si la Partie requise a besoin d'éclaircissements sur la demande ou exige des informations supplémentaires pour donner suite à la demande, elle devrait consulter le Point de Contact du Réseau 24/7 de la Partie requérante.

165. En application du paragraphe 3.g, la demande précise toute instruction procédurale spéciale. Il s'agit notamment des demandes particulières de non-divulgation de la demande aux abonnés et autres tiers ou des formulaires d'authentification à remplir pour les données recherchées. En vertu de ce paragraphe, ces instructions de procédure sont fournies dès le départ, car des instructions spéciales peuvent entraîner des processus supplémentaires chez la Partie requise. Dans certaines Parties, la confidentialité peut être préservée par application de la loi, alors que dans d'autres Parties, ce n'est pas nécessairement le cas. Par conséquent, afin d'éviter le risque de divulgation prématurée de l'enquête, les Parties sont encouragées à communiquer sur la nécessité de préserver la confidentialité et les difficultés qui pourraient se poser, préciser les éventuelles lois applicables, ainsi que les politiques d'un fournisseur de services concernant la notification. Étant

donné que les demandes d'authentification des données en réponse à une demande peuvent souvent ralentir le processus alors que l'objectif clé est la divulgation rapide des données recherchées, les autorités de la Partie requise devraient déterminer, en consultation avec les autorités de la Partie requérante, quand et de quelle manière la confirmation de l'authenticité doit être donnée.

166. En outre, la Partie ou le fournisseur de services peut exiger des informations supplémentaires pour localiser et divulguer les données informatiques stockées recherchées par la Partie.

Paragraphe 4

167. Le paragraphe 4 exige que la Partie requise accepte les demandes sous forme électronique. Les Parties sont encouragées à utiliser des moyens de communication rapides pour faciliter la transmission d'informations ou de données et de documents, y compris la transmission des demandes. Ce paragraphe est basé sur le paragraphe 5 de l'Article 8 mais il a été modifié pour ajouter qu'une Partie peut accepter des demandes oralement, une méthode de communication fréquemment utilisée par le réseau 24/7.

Paragraphe 5

168. Le paragraphe 5 permet à une Partie de déclarer qu'elle exige que d'autres Parties qui lui demandent des données conformément au présent article fournissent, après l'exécution de la demande et transmission des données, la demande et toute information supplémentaire transmise à l'appui de celle-ci, dans un format spécifique et par le biais d'un canal spécifique. Par exemple, une Partie peut déclarer que dans des circonstances spécifiques, elle demandera à une Partie requérante que cette dernière soumette subséquemment une demande d'entraide judiciaire afin de justifier formellement la demande d'urgence et la divulgation des données. Pour certaines Parties, une telle procédure serait exigée par leurs lois nationales, tandis que d'autres Parties ont indiqué qu'elles n'ont pas de conditions de ce type et n'ont pas à se prévaloir de cette possibilité de déclaration.

Paragraphe 6

169. Le présent article fait référence à des « demandes » et n'exige pas que les Parties requises fournissent les données demandées aux Parties requérantes. Par conséquent, les rédacteurs reconnaissent qu'il y aura des situations dans lesquelles les Parties requises ne fourniront pas les données demandées à une Partie requérante en vertu du présent article. La Partie requise peut déterminer que, dans un cas particulier, une entraide d'urgence en vertu de l'article 10 ou un autre moyen de coopération serait le plus approprié. Par conséquent, le paragraphe 6 prévoit que lorsqu'une Partie requise détermine qu'elle ne fournira pas les données demandées à une Partie qui a fait une demande en vertu du paragraphe 1 du présent article, la Partie requise informe la Partie requérante de sa décision rapidement et, le cas échéant, précise les conditions dans lesquelles elle fournirait les données et explique toute autre forme de coopération qui pourrait être disponible, afin d'atteindre l'objectif mutuel des Parties d'accélérer la divulgation des données en cas d'urgence.

Paragraphe 7

170. Le paragraphe 7 décrit les procédures applicables lorsque l'État requis a spécifié les conditions dans lesquelles il accède à la demande de coopération qui lui a été adressée en vertu du paragraphe 6. Si la partie requérante ne peut pas se conformer à ces conditions, le paragraphe 7.a lui impose d'en informer rapidement la Partie requise, qui décidera alors si l'assistance demandée peut tout de même être accordée. En revanche, lorsque la Partie requérante accepte une condition spécifique, elle est tenue de la respecter. En vertu du paragraphe 7.b, une Partie requise qui a transmis des renseignements ou du matériel sous réserve d'une condition fixée en application du

paragraphe 6 peut, afin de pouvoir contrôler le respect de cette condition, exiger que la Partie requérante explique l'usage qui a été fait des renseignements ou du matériel transmis, mais il a été entendu que la Partie requérante ne peut pas exiger une comptabilité trop lourde. (Voir Rapport explicatif, paragraphes 279 et 280 de la Convention).

Section 4 – Procédures relatives à l'entraide d'urgence

Article 10 – Entraide d'urgence

171. L'article 10 du protocole a pour but de prévoir une procédure qui soit rapide pour les demandes d'entraide effectuées en situation d'urgence. Une situation d'urgence est définie à l'article 3, paragraphe 2.c et expliquée dans les paragraphes correspondants 41 et 42 du présent rapport explicatif.

172. Étant donné que l'article 10 de ce Protocole est limité aux urgences justifiant une telle célérité dans l'action, il est distinct de l'article 25, paragraphe 3 de la Convention, qui prévoit que les demandes d'entraide peuvent être transmises par des moyens de communication rapides en situations d'urgence qui ne sont pas du niveau d'urgence défini. En d'autres termes, l'article 25, paragraphe 3, a une portée plus large que l'article 10 du Protocole puisqu'il couvre des situations non couvertes par ce dernier, par exemple les risques existants mais non imminents pour la vie ou la sécurité de personnes physiques, la destruction potentielle de preuves qui pourrait résulter d'un retard, le fait que la date d'un procès se rapproche ou autres types d'urgences. Alors que le mécanisme visé à l'article 25, paragraphe 3, prévoit une méthode plus rapide pour transmettre une demande et y répondre, les obligations en cas d'urgence relevant de l'article 10 du Protocole sont nettement plus lourdes; en d'autres termes, lorsqu'il existe un risque significatif et imminent pour la vie ou la sécurité d'une personne physique, le processus devrait être encore plus rapide. (Voir paragraphe 42 du présent rapport explicatif ci-dessus pour des exemples de situations d'urgence).

Paragraphe 1

173. En vertu du paragraphe 1, lorsqu'elle présente une demande d'urgence, la Partie requérante doit à la fois conclure qu'il existe une urgence au sens de l'article 3, paragraphe 2.c, et inclure dans sa demande une description des faits tendant à le démontrer et expliquer comment l'entraide sollicitée est nécessaire pour répondre à la situation urgente, en plus des informations qui doivent figurer dans la demande en vertu du traité applicable ou du droit interne de la Partie requise. A cet égard, il convient de rappeler qu'au titre de l'article 25, paragraphe 4 de la Convention, l'exécution des demandes d'entraide judiciaire, y compris urgentes, est en général « soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération ». Les rédacteurs ont compris que cela s'appliquait également aux demandes d'entraide d'urgence au titre du présent protocole.

Paragraphe 2

174. Le paragraphe 2 exige de la Partie requise qu'elle accepte la demande d'entraide sous forme électronique. Avant d'accepter la demande, la Partie requise peut conditionner son acceptation au respect par la Partie requérante de niveaux de sécurité et d'authentification appropriés. Pour ce qui est de la condition de sécurité prévue dans ce paragraphe, les Parties peuvent décider d'un commun accord s'il est nécessaire d'établir des protections de sécurité spéciales (dont le cryptage) en cas d'affaire particulièrement sensible.

Paragraphe 3

175. Lorsque la Partie requise demande un complément d'informations pour étayer la situation urgente au sens de l'Article 3, paragraphe 2.c, et/ou que les autres conditions liées à la demande

d'entraide ont été remplies, le paragraphe 3 prévoit que ce complément d'informations doit être demandé de manière accélérée. Réciproquement, le paragraphe 3 exige de la Partie requérante qu'elle communique le complément d'informations avec la même célérité. Les deux Parties doivent donc faire leur maximum pour éviter toute perte de temps qui pourrait involontairement entraîner une issue tragique.

Paragraphe 4

176. En vertu du paragraphe 4, une fois que les informations nécessaires à l'exécution de la demande ont été communiquées, il est demandé à la Partie requise d'exécuter la demande urgente avec la même célérité. En général, cela signifie d'obtenir d'urgence les mandats judiciaires obligeant le fournisseur à produire les données qui prouvent l'infraction et de faire procéder d'urgence à la signification de l'injonction au fournisseur. Cependant, les autorités de la Partie requise ne sauraient être tenues responsables des retards occasionnés par les délais de réponse du fournisseur à ces injonctions.

Paragraphe 5

177. En vertu du paragraphe 5, toutes les Parties veillent à ce que des membres de leur autorité centrale ou d'autres autorités responsables des demandes d'entraide soient joignables 24 heures sur 24, sept jours sur sept, pour recevoir des demandes d'entraide urgentes qui parviendraient en-dehors des heures ouvrables. Il convient de rappeler qu'à cet égard, le réseau 24/7 créé au titre de l'article 35 de la Convention-mère est disponible pour se coordonner avec les autorités responsables de l'entraide. L'obligation prévue dans ce paragraphe n'exige pas de l'autorité centrale ou des autres autorités responsables des demandes d'entraide qu'elle(s) prévoie(nt) un personnel d'astreinte à tout moment. En revanche, elle devrait prendre des mesures pour garantir que des membres de son personnel sont joignables en-dehors des heures ouvrables pour examiner des demandes urgentes. Le T-CY s'efforcera de manière informelle de tenir un répertoire de ces autorités.

Paragraphe 6

178. Le paragraphe 6 offre une base qui permet aux autorités centrales et aux autres autorités responsables de l'entraide de s'entendre sur un canal alternatif de transmission des informations demandées ou de la preuve; il peut s'agir du mode de transmission ou des autorités entre lesquelles s'opère la transmission. Ainsi, plutôt que de renvoyer les informations ou preuves demandées par le biais de l'autorité centrale habituellement utilisée pour la transmission des informations prévues ou des preuves aux fins de l'exécution de la demande par la Partie requérante, elles peuvent alors décider d'utiliser un canal différent pour accélérer la transmission, préserver l'intégrité de la preuve ou pour toute autre raison. Par exemple, en cas d'urgence, les autorités peuvent décider de la transmission des preuves directement à une autorité d'enquête ou de poursuite de la Partie requérante qui les utilisera, plutôt que de les transmettre via la chaîne des autorités qui se chargent en temps normal de les acheminer. Les autorités peuvent aussi, par exemple, déterminer un traitement spécial de preuves matérielles pour être à même d'écarter dans les procédures judiciaires ultérieures les contestations au motif que la preuve aurait pu avoir été altérée ou contaminée, ou peuvent décider ensemble d'un traitement spécial de la transmission de preuves sensibles.

Paragraphe 7

179. S'agissant des procédures visées à cet article, il existe deux possibilités, décrites aux paragraphes 7 et 8. Le paragraphe 7 dispose que les Parties concernées, lorsqu'elles ne sont pas liées par un accord d'entraide en vigueur, ou par un accord d'entraide applicable sur la base d'une législation uniforme ou réciproque, appliquent certaines procédures définies aux paragraphes visés des articles 27 et 28 de la Convention (régissant l'entraide en l'absence d'un traité).

Paragraphe 8

180. En vertu du paragraphe 8, lorsque les Parties concernées sont liées par un tel accord ou arrangement, cet article est complétée par les dispositions de cet accord, à moins que les Parties concernées décident d'un commun accord d'appliquer tout ou partie des dispositions de la Convention visées au paragraphe 7 en lieu et place dudit accord.

Paragraphe 9

181. Enfin, le paragraphe 9 prévoit la possibilité d'une déclaration par laquelle les Parties au présent Protocole peuvent prévoir que les demandes peuvent être faites directement entre les procureurs ou autres autorités judiciaires. Dans certaines Parties, ces voies de communication directes entre autorités judiciaires sont bien établies et peuvent constituer un moyen efficace d'accélérer encore la présentation et l'exécution des demandes. La transmission de la demande d'urgence par le point de contact de la Partie 24 heures sur 24 et 7 jours sur 7 ou par l'Organisation internationale de police criminelle (INTERPOL) est utile non seulement pour réduire tout retard mais aussi pour renforcer les normes de sécurité et d'authentification. Toutefois, dans certaines Parties, l'envoi d'une demande directement à une autorité judiciaire de la Partie requise sans l'intervention et l'approbation de son autorité centrale pourrait être contre-productif dans la mesure où, sans les conseils et/ou l'approbation de l'autorité centrale, l'autorité destinataire peut ne pas être habilitée à agir de manière indépendante, ou peut ne pas être familiarisée avec la procédure appropriée. Par conséquent, une partie doit déclarer que les demandes peuvent être envoyées par ces canaux d'autorité non centrale.

Section 5 – Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

182. Comme le prévoit l'article 5, paragraphe 5, la présente section, relative aux articles 11 et 12, s'applique « lorsqu'il n'existe pas de traité ou d'arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les Parties requérante et requise. Les dispositions de la section 5 ne s'appliquent pas lorsqu'un tel traité ou arrangement existe, sauf dans les cas prévus à l'article 12, paragraphe 7. Toutefois, les Parties concernées peuvent décider d'un commun accord d'appliquer la section 5 en lieu et place de celle-ci, si le traité ou l'arrangement ne l'interdit pas ». Ceci suit l'approche de l'article 27 de la Convention.

183. Entre certaines Parties à ce Protocole, les sujets des articles 11 et 12 sont déjà réglementés par les termes des traités d'entraide (par exemple, le deuxième Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale (STE n° 182); ou l'Accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique). D'autres traités d'entraide, tels que le STE n° 182, peuvent également fournir plus de détails sur les circonstances dans lesquelles une telle coopération peut avoir lieu, ainsi que sur les conditions et les procédures qui la régissent.

184. Bien que les rédacteurs aient examiné ces traités, les articles 11 et 12 du présent Protocole contiennent des termes qui diffèrent des dispositions analogues figurant dans d'autres traités d'entraide.

185. Bien que les termes de la STE n° 182 continueront à être appliqués entre les Parties à celle-ci, il a été jugé approprié de réglementer ces deux articles dans le présent Protocole d'une manière qui diffère à certains égards pour les raisons suivantes:

- La composition du STE n° 182 est différente de celle de la Convention sur la cybercriminalité et ses dispositions ne sont donc pas disponibles pour la coopération entre toutes les Parties à la Convention sur la cybercriminalité. Le STE n° 182 a été négocié pour répondre aux besoins des États membres du Conseil de l'Europe plutôt qu'aux exigences, systèmes et

besoins juridiques de toutes les Parties à la Convention sur la cybercriminalité, bien que, en principe, la Convention européenne d'entraide judiciaire en matière pénale (STE n° 30) et ses Protocoles soient ouverts à l'adhésion des États non-membres du Conseil de l'Europe à la suite d'une invitation du Comité des Ministres.

- Les dispositions du présent Protocole relatives à l'entraide judiciaire ont un champ d'application matériel spécifique en ce sens qu'elles s'appliquent aux « enquêtes ou procédures pénales spécifiques concernant les infractions pénales liées aux systèmes et données informatiques, ainsi qu'à la collecte de preuves sous forme électronique d'une infraction pénale » (Article 2). Compte tenu des problèmes particuliers de ce type d'enquêtes ou de procédures - tels que la volatilité des données, les questions liées à la territorialité et à la compétence, et au volume des demandes - les dispositions analogues de la STE n° 182 ne sont pas toujours applicables de la même manière.

- Les rédacteurs ont reconnu que « puisque la Convention s'applique à des Parties ayant des systèmes juridiques et des cultures très différents, il n'est pas possible de préciser en détail les conditions et les garanties applicables à chaque pouvoir ou procédure ». (Voir paragraphe 145 du rapport explicatif de la Convention). En revanche, les Parties sont tenues de veiller à assurer « une protection adéquate des droits de l'homme et des libertés » et à appliquer « des normes communes [et] des garanties minimales auxquelles les Parties ... doivent adhérer », y compris « les garanties découlant des obligations qu'une Partie a contractées en vertu des instruments internationaux relatifs aux droits de l'homme applicables » (voir le rapport explicatif, paragraphe 145 de la Convention). Voir l'article 13 du présent Protocole (incorporant l'article 15 de la Convention). Par conséquent, contrairement aux dispositions de la STE n° 182 - par exemple, l'article 9 sur l' « audition par vidéoconférence » - qui prescrivent des procédures et des garanties spécifiques à suivre par les Parties à la STE n° 182, les dispositions correspondantes du présent Protocole permettent une plus grande souplesse dans la mise en œuvre par les Parties. Par exemple, les procédures et conditions régissant le fonctionnement des équipes communes d'enquête doivent être convenues entre les autorités compétentes des Parties (voir article 12, paragraphe 2), et en ce qui concerne la vidéoconférence, une Partie requise peut exiger des conditions et garanties particulières lorsqu'elle autorise l'audition d'un suspect ou d'une personne poursuivie par vidéoconférence (voir Article 11, paragraphe 7). Dans la mesure prévue par ces articles, les Parties peuvent également décider de ne pas coopérer si leurs exigences en matière de conditions et de garanties ne sont pas satisfaites.

186. Les articles 11 et 12 du présent Protocole ne s'appliquent qu'en l'absence d'autres traités ou arrangements d'entraide sur la base de législations uniformes ou réciproques - à moins que les parties concernées ne décident d'un commun accord d'appliquer tout ou partie de leurs dispositions à la place de celles-ci, si le traité ou l'arrangement ne l'interdit pas. Toutefois, l'article 12, paragraphe 7, s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les parties concernées.

Article 11 – Vidéoconférence

187. L'article 11 concerne avant tout le recours à la technologie de la vidéoconférence pour recueillir des dépositions. Cette forme de coopération peut être prévue dans des traités d'entraide judiciaire bilatéraux et multilatéraux, par exemple dans le STE 182 (Deuxième Protocole additionnel à la Convention d'entraide judiciaire en matière pénale). Pour ne pas se substituer à des dispositions spécifiquement conçues pour répondre aux besoins des parties à ces traités ou conventions, et comme indiqué dans les principes généraux applicables à la présente section (Article 5, paragraphe 5), l'Article 11, comme l'article 12 du présent Protocole « s'applique en l'absence de traité sur l'entraide judiciaire, ou d'arrangements sur la base de l'uniformité ou de la réciprocité législatives, en vigueur entre les Parties requérante et requise. Les dispositions de la section 5 ne sont pas applicables lorsqu'un tel traité ou arrangement existe, sauf dans les cas prévus à l'article 12,

paragraphe 7. Toutefois, les parties concernées peuvent convenir de déterminer d'un commun accord d'appliquer les dispositions de la section 5 en lieu et place de celles-ci, si le traité ou l'arrangement ne l'interdit pas ».

Paragraphe 1

188. Le paragraphe 1 autorise le recueil de dépositions d'un témoin ou expert par le recours à la vidéoconférence. Il laisse à la Partie requise toute latitude pour accepter ou non la demande d'entraide ou pour fixer des conditions à son assistance. Par exemple, une Partie peut refuser ou remettre à ultérieurement de fournir une assistance pour les motifs prévus à l'Article 27, paragraphes 4 et 5 de la Convention. Par ailleurs, lorsqu'il serait plus efficace que l'assistance soit fournie d'une manière différente, par exemple au moyen d'un formulaire écrit authentifiant des documents officiels ou commerciaux, la Partie requise peut choisir de fournir l'assistance de cette manière.

189. Dans le même temps, il est attendu des Parties au Protocole qu'elles disposent de la capacité technique de base pour exécuter la demande d'entraide au moyen de la vidéoconférence.

190. Utiliser la vidéoconférence pour recueillir une déposition peut poser de nombreuses difficultés, notamment de nature juridique, logistique ou technique. Pour que la vidéoconférence fonctionne sans heurts, il est essentiel de se coordonner par avance et parfois durant l'opération si la Partie requise pose des conditions préalables à la vidéoconférence. Le paragraphe 1 exige donc aussi que les Parties requérante et requise se concertent au besoin pour faciliter la résolution de tout problème de ce type qui pourrait se poser. Par exemple, comme expliqué plus avant, la vidéoconférence peut devoir suivre une certaine procédure pour que les éléments recueillis soient admissibles en tant que preuve devant les juridictions de la Partie requérante. Il se peut aussi que la Partie requise ait besoin d'appliquer ses propres conditions juridiques à certains égards (par exemple pour une prestation de serment du témoin ou la notification de ses droits à ce dernier). De plus, la Partie requise peut exiger que son ou ses représentants des services concernés soient présents à la vidéoconférence dans certains ou dans tous les cas, qu'ils puissent contrôler la procédure ou veiller à ce que les droits de la personne dont on recueille la déposition soient respectés. A cet égard, il peut ressortir des consultations que certaines Parties requises exigent que leur représentant à la vidéoconférence puisse intervenir, interrompre ou mettre un terme à l'audition s'il y a des doutes quant à la conformité avec les dispositions de son droit interne, alors que d'autres Parties peuvent autoriser la tenue d'une vidéoconférence sans participation d'un représentant dans certains cas. Autre exemple, des Parties requises peuvent envisager des garanties spécifiques concernant les témoins menacés, les enfants témoins, etc. Ces questions doivent être discutées et décidées à l'avance. Dans certains cas, le souhait de la Partie requise de mener une seule procédure peut aller à l'encontre des dispositions légales de la Partie requérante ayant pour objectif de faciliter l'utilisation de la déposition durant le procès. En de tels cas, les Parties devraient faire leur maximum pour tenter de trouver des solutions créatives répondant aux impératifs de chacune. De plus, les Parties devraient se consulter à l'avance pour faciliter la résolution des problèmes tels que la manière de répondre aux objections ou revendications de privilège ou d'immunité de la part de la personne concernée ou de son avocat, ou encore la manière d'utiliser des preuves documentaires ou autres durant la vidéoconférence. Il est aussi possible que des procédures particulières soient nécessaires du fait de conditions posées à la tenue de la vidéoconférence. Des questions logistiques, par exemple savoir qui, de la Partie requérante ou de la Partie requise, devrait assurer l'interprétation et l'enregistrement de la déposition, devraient aussi être discutées; la coordination technique devrait aussi être abordée pour régler les modalités relatives au démarrage et au maintien de la transmission, ainsi que pour disposer de canaux alternatifs de communication si la transmission est interrompue.

Paragraphe 2

191. Le paragraphe 2 traite de plusieurs aspects d'ordre procédural et apparenté régissant cette forme de coopération (outre les autres procédures et conditions applicables exposées dans les autres paragraphes de cet article), qui ont été repris ou adaptés de la Convention. Le paragraphe 2 se subdivise en deux sous-paragraphes.

192. La vidéoconférence constituant une forme d'entraide, le paragraphe 2.a dispose que les autorités centrales des Parties requises et requérantes communiquent directement entre elles aux fins de l'application de cet article. Cet article s'appliquant uniquement en l'absence d'un accord ou d'un arrangement d'entraide sur la base d'une législation uniforme ou réciproque, on entend ici par « autorité centrale » l'autorités ou les autorités désignées en vertu de l'article 27, paragraphe 2.a, de la Convention. Voir l'article 3, paragraphe 2.a, et le paragraphe 38 du Rapport explicatif.

193. Le paragraphe 2.a prévoit aussi qu'une Partie requise accepte une requête de vidéoconférence sous forme électronique et qu'elle puisse exiger des niveaux de sécurité et d'authentification appropriés avant d'accepter cette demande.

194. Le paragraphe 2.b (de même que l'article 27, paragraphe 7, de la Convention) impose à la Partie requise d'informer la Partie requérante des raisons pour lesquelles elle n'a pas exécuté la demande ou tardé à l'exécuter. Comme indiqué au paragraphe 192 ci-dessus, ces communications doivent passer par des autorités centrales. Enfin, le paragraphe 2.b prévoit que l'article 27, paragraphe 8 (relatif à la confidentialité d'une demande d'entraide en l'absence d'un traité) et l'article 28, paragraphes 2 à 4 (relatifs à la confidentialité de la réponse et à l'imposition de conditions restrictives en l'absence d'un traité), de la Convention s'appliquent à la vidéoconférence.

Paragraphe 3

195. Étant donné que pour une vidéoconférence, il se peut que des personnels judiciaires et auxiliaires de justice de la Partie requérante doivent être disponibles pour participer au recueil de la déposition dans la Partie requise, qui peut se trouver à plusieurs fuseaux horaires de distance de la Partie requérante, il faut absolument que la personne auditionnée soit sur place à l'heure dite. En vertu du paragraphe 3, lorsque la Partie requise prête son concours au titre du présent article, elle doit faire tout son possible pour obtenir la comparution de la personne dont la déposition est requise. Les solutions les plus appropriées peuvent être tributaires des circonstances de l'affaire, ou du cadre de la loi nationale de la Partie requise; la question peut également se poser du degré de confiance à accorder à la comparution volontaire de la personne au moment prévu. En revanche, pour garantir la comparution de la personne, il peut être souhaitable que la Partie requise délivre une injonction ou une citation à comparaître, et ce paragraphe l'y autorise, conformément aux garanties prévues par son droit interne.

Paragraphe 4

196. La procédure pour mener les vidéoconférences est exposée au paragraphe 4. L'objectif essentiel consiste à fournir la déposition à la Partie requérante sous une forme qui lui permettra de s'en servir comme preuve dans son enquête et sa procédure. C'est pourquoi ce sont les procédures demandées par la Partie requérante qui seront suivies, à moins qu'elles ne soient contraires aux dispositions légales de la Partie requise, notamment aux principes juridiques applicables dans la Partie requise qui ne sont pas codifiés dans sa législation. Ainsi, durant la vidéoconférence, il s'agirait de privilégier la procédure selon laquelle la Partie requise autorise les autorités de la Partie requérante à interroger directement la personne dont on veut obtenir la déposition. Cette tâche incombera au procureur, juge d'instruction ou enquêteur de la Partie requérante, qui connaît le mieux l'enquête pénale ou les poursuites et est donc le mieux placé pour savoir quelles sont les questions à poser qui seront les plus utiles à l'enquête ou aux poursuites ainsi que la meilleure manière de les poser pour se conformer au droit de la Partie requérante. Dans ce cas, l'autorité de

la Partie requise participant à l'audition n'interviendra que si cela est nécessaire du fait que l'autorité de la Partie requérante a eu un comportement incompatible avec le droit de la Partie requise. Elle pourra alors réfuter des questions, reprendre elle-même l'interrogatoire ou procéder à tout acte approprié en vertu de son droit et des circonstances dans lesquelles se déroule la vidéoconférence. L'expression « incompatible avec le droit de la Partie requise » ne couvre pas des situations dans lesquelles la procédure est simplement différente de celle qui a cours dans la Partie requise, ce qui sera souvent le cas. Elle vise plutôt des situations dans lesquelles la procédure est contraire au droit de la Partie requise ou ne peut pas fonctionner dans ce cadre. En un tel cas, ou si la Partie requérante n'a pas demandé de procédure spécifique, la procédure par défaut sera celle qui s'applique dans le droit interne de la Partie requise. Si l'application du droit de la Partie requise pose problème à la Partie requérante, par exemple pour ce qui est de l'admissibilité de la déposition lors du procès, les Parties requérante et requise peuvent chercher à s'entendre sur une procédure différente qui satisfera la Partie requérante tout en évitant le problème potentiel dans le droit interne de la Partie requise.

Paragraphe 5

197. Le paragraphe 5, qui concerne la peine ou sanction applicable pour faux témoignage, refus de répondre et autres comportements répréhensibles, a pour but de protéger l'intégrité du processus de recueil d'une déposition lorsque le témoin se trouve physiquement dans un autre pays que celui où se déroule la procédure pénale. Dans la mesure où la Partie requise a fait obligation à la personne entendue de témoigner, de dire toute la vérité, ou qu'elle lui a interdit certains comportements (notamment le fait de perturber la procédure), la personne entendue subira la conséquence de ses actes prévue dans la juridiction où elle se trouve. En de tels cas, la Partie requise doit pouvoir appliquer la sanction qu'elle appliquerait si le comportement répréhensible s'était produit dans le cadre de l'une de ses procédures nationales. La sanction s'applique sans préjudice d'une éventuelle compétence de la Partie requérante. Cette condition est une incitation supplémentaire pour que le témoin témoigne, témoigne sincèrement et ne se livre pas à un comportement répréhensible. Si aucune sanction n'est prévue dans les procédures en droit interne de la Partie requise (par exemple pour faux témoignage par une personne inculpée), il n'est pas demandé d'en prévoir une pour un tel comportement commis durant une vidéoconférence. Cette disposition sera particulièrement utile pour permettre de poursuivre un témoin faisant un faux témoignage mais qui ne peut être extradé pour être poursuivi dans la Partie requérante du fait par exemple que la Partie requise interdit l'extradition de ses ressortissants.

Paragraphe 6

198. Le paragraphe 6 prévoit des règles concernant la couverture des frais liés à des vidéoconférences. De manière générale, les frais engendrés dans le cadre d'une vidéoconférence sont supportés par la Partie requise, sauf pour ce qui concerne (1) les honoraires d'un témoin expert; (2) les frais de traduction, d'interprétation et de transcription, et (3) des coûts si élevés qu'ils en deviennent exceptionnels. Les frais de voyage et d'hébergement dans la Partie requise sont la plupart du temps négligeables et en général couverts par cette dernière. Les règles en matière de couverture des coûts peuvent cependant être modifiées d'un commun accord entre les Parties requérante et requise. Ainsi, si la Partie requérante prévoit que la présence d'un interprète sera nécessaire ou qu'il faudra des services de transcription à la fin de la vidéoconférence, il est possible que la Partie requise ne paie pas pour la prestation de ces services. Quand la Partie requise prévoit des frais exceptionnels pour la fourniture de l'entraide, conformément au paragraphe 6.b), la Partie requérante et la Partie requise se concertent préalablement à l'exécution de la demande pour déterminer si la Partie requérante peut supporter ces frais et, en cas contraire, comment les éviter.

Paragraphe 7

199. Si le paragraphe 1 autorise expressément l'utilisation de la technologie de vidéoconférence pour le recueil d'une déposition, paragraphe 7.a) prévoit que les dispositions de l'article 11 peuvent

sur consentement mutuel être appliquées aux fins de la réalisation d'une vidéoconférence. De plus, le paragraphe 7.b) prévoit que, sur consentement mutuel des Parties requérante et requise, la technologie peut être utilisée à d'autres « fins, pour des auditions … par exemple l'identification de personnes ou d'objets ». Ainsi, si elles en sont convenues, les Parties requérante et requise peuvent envisager d'utiliser la technologie de vidéoconférence pour auditionner ou mener des procédures concernant un suspect ou un inculpé (on relèvera que certaines Parties peuvent considérer qu'un suspect ou un inculpé est un « témoin », de sorte que le recueil de sa déposition serait déjà couvert par les dispositions du paragraphe 1 du présent article). Si le paragraphe 1 n'est pas applicable, il est possible de s'appuyer juridiquement sur le paragraphe 6 pour autoriser l'utilisation de cette technologie dans ces cas-là.

Paragraphe 8

200. Le paragraphe 8 traite la situation dans laquelle la Partie requise choisit d'autoriser l'audition d'un suspect ou inculpé par exemple pour recueillir une déposition ou des déclarations, ou aux fins de notifications ou pour d'autres mesures procédurales. Tout comme la Partie requise a toute latitude pour autoriser l'utilisation de la vidéoconférence en vue d'entendre un témoin ordinaire ou expert, elle peut en faire de même pour ce qui est d'entendre un suspect ou un inculpé. De plus, outre toute autre condition ou limitation qu'une Partie requise peut imposer pour autoriser la tenue d'une vidéoconférence, le droit interne d'une Partie peut prévoir des conditions particulières concernant l'audition de suspects ou d'inculpés et par exemple imposer le consentement du suspect ou de l'inculpé préalablement à l'audition, ou encore interdire ou limiter l'utilisation de la vidéoconférence pour les notifications ou autres mesures procédurales. Le paragraphe 8 est donc conçu pour insister sur le fait que les procédures visant un suspect ou un inculpé peuvent entraîner la nécessité de mettre en place des conditions ou garanties en complément de celles qui s'appliqueraient par ailleurs.

Article 12 – Équipes communes d'enquête et enquêtes communes

201. La cybercriminalité et la preuve électronique étant par nature transnationales, les enquêtes et poursuites qui y sont relatifs présentent souvent des liens avec d'autres États. Les équipes communes d'enquête (ECE) peuvent être un moyen efficace de coopération ou coordination opérationnelles entre deux États ou plus. L'article 12 donne une base pour de telles formes de coopération.

202. L'expérience a montré que lorsqu'un État enquête sur une infraction ayant une dimension transfrontalière en lien avec la cybercriminalité ou pour laquelle il faut obtenir des preuves électroniques, l'enquête peut tirer parti de la participation des autorités d'autres États qui sont également en train d'enquêter sur les mêmes actes criminels ou des actes connexes, ou bénéficier utilement d'une coordination.

203. Comme indiqué dans l'article 5 du présent Protocole et les paragraphes 182 à 186 du rapport explicatif, les dispositions du présent article ne s'appliquent pas en présence d'un traité d'entraide judiciaire ou d'un arrangement sur la base de dispositions législatives uniformes ou réciproques en vigueur entre les Parties requérante et requise, à moins que les Parties concernées ne conviennent d'appliquer tout ou partie du reste de cet article en leur lieu et place , si le traité ou l'arrangement ne l'interdit pas. Comme expliqué ci-dessous, le paragraphe 7 s'applique qu'il existe ou non un traité ou un arrangement d'entraide sur la base des législations uniformes ou réciproques en vigueur entre les parties concernées.

Paragraphe 1

204. Le paragraphe 1 prévoit que les autorités compétentes de deux Parties ou plus peuvent convenir d'établir une ECE lorsqu'elles l'estiment particulièrement utile. La participation à une ECE se fait par accord mutuel. Les termes « commun accord », « accord » et « convenir » – tels

qu'utilisés dans cet article – ne doivent pas être compris comme comprenant la nécessité d'un accord contraignant au sens du droit international.

205. Le présent article utilise deux expressions liées: « autorités compétentes » et « autorités participantes ». Chaque Partie détermine quelles sont les autorités compétentes – les « autorités compétentes » – pour conclure un accord établissant une ECE. Certaines Parties peuvent y autoriser un ensemble de fonctionnaires tels que des procureurs, des juges d'instruction ou également des officiers de police de haut rang dirigeant des enquêtes ou procédures pénales à participer à ce type d'accord; d'autres peuvent autoriser l'autorité centrale – le service normalement responsable des questions d'entraide – à le faire. De même, la détermination des autorités qui participent effectivement à une ECE – les « autorités participantes » – relève respectivement des Parties concernées.

Paragraphe 2

206. Le paragraphe 2 prévoit que les procédures et modalités régissant le fonctionnement des équipes communes d'enquête, telles que leurs objectifs spécifiques, leur composition; leurs fonctions; leur durée et toute éventuelle prolongation; leur emplacement; leur organisation; les conditions de recueil, de transmission et d'utilisation des informations ou preuves; les conditions de confidentialité; et les conditions de l'implication des autorités participantes d'une Partie dans des mesures d'enquête se déroulant sur le territoire d'une autre Partie, feront l'objet d'un accord entre les autorités compétentes concernées. En particulier, lorsqu'elles discutent du contenu à donner à l'accord, les Parties concernées peuvent souhaiter établir des critères de refus ou de restriction de l'utilisation des informations et preuves y compris, par exemple, pour les motifs établis aux paragraphes 4 ou 5 de l'article 27 de la Convention, et préciser la procédure à suivre si ces dernières sont nécessaires pour des finalités autres que celles qui avaient présidé à l'établissement de l'accord (y inclus l'utilisation des informations ou preuves par le ministère public ou la défense dans une autre affaire ou leur utilisation pour prévenir une situation d'urgence telle que définie à l'article 3, paragraphe 2.c, c'est-à-dire présentant un risque significatif et imminent pour la vie ou la sécurité d'une personne physique). Les Parties sont encouragées à spécifier dans l'accord les limites des pouvoirs des personnes habilitées participantes d'une Partie qui sont physiquement présentes sur le territoire d'une autre Partie. Les Parties sont également encouragées à permettre dans l'accord la transmission électronique des informations ou preuves recueillies.

207. Il est supposé que les Parties établissent généralement par écrit ces procédures et conditions. Dans tout accord, il conviendrait de tenir compte du niveau de détail requis. Un texte standardisé peut présenter le niveau de précision nécessaire pour des situations prévisibles, avec la possibilité d'ajouter des dispositions supplémentaires si les circonstances exigeaient davantage de précisions. Les Parties prendront en compte le champ d'application territorial et la durée de l'accord établissant l'ECE et le fait que l'accord pourrait nécessiter d'être modifié ou étendu en cas de faits nouveaux.

208. Les informations ou preuves utilisées dans le cadre de l'équipe commune d'enquête peuvent inclure des données à caractère personnel sous la forme de données relatives aux abonnés, de données de trafic ou de données de contenu. Comme pour d'autres mesures de coopération couvertes par le Protocole, l'article 14 s'applique au transfert de données à caractère personnel dans le cadre d'ECE.

209. Comme c'est généralement le cas pour toutes informations ou preuves reçues par une Partie en vertu du Protocole, les règles de la preuve applicables dans son droit interne régiront l'admissibilité des informations ou preuves dans les procédures judiciaires.

Paragraphe 3

210. Le paragraphe 3 permet à une Partie de déclarer, au moment de sa signature de ce Protocole ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, que son autorité centrale doit être signataire de l'accord portant création de l'équipe ou y souscrire d'une autre manière. Cette disposition a été insérée pour plusieurs raisons. Tout d'abord, plusieurs Parties considèrent que les ECE constituent une forme d'entraide. De plus, dans plusieurs autres Parties, les autorités centrales chargées de l'entraide peuvent avoir un rôle à jouer pour garantir que les conditions de droit interne applicables sont remplies lorsque les autorités compétentes (qui peuvent être des procureurs ou des services de police à l'expérience relativement limitée en matière de coopération internationale) préparent un accord établissant une ECE en vertu de cet article. L'expérience d'une autorité centrale en matière d'accords internationaux régissant l'entraide et d'autres formes de coopération internationale (y compris aux termes du présent Protocole) peut aussi l'aider à jouer un rôle précieux pour garantir le respect des conditions fixées par le Protocole. Enfin, lorsqu'une Partie a fait une déclaration en vertu de ce paragraphe, les autorités des autres Parties souhaitant établir une ECE avec la partie déclarante savent que l'autorité centrale de la Partie déclarante doit signer l'accord établissant l'ECE ou y souscrire d'une autre manière afin que cet accord soit valide en vertu du Protocole. Cette disposition empêche la conclusion d'un accord établissant une ECE qui n'aurait pas reçu l'autorisation requise ou qui ne serait pas conforme aux conditions légales applicables de la Partie déclarante.

Paragraphe 4

211. En vertu du paragraphe 4, les autorités compétentes déterminées par les Parties en vertu du paragraphe 1 et les autorités participantes visées au paragraphe 2 communiqueront en principe directement entre elles dans un souci d'efficience et d'efficacité. Cependant, si des circonstances exceptionnelles exigent une coordination plus centrale – par exemple dans des affaires présentant des ramifications particulièrement graves ou des situations présentant des problèmes particuliers de coordination -, il peut être convenu d'autres canaux appropriés. Ainsi, les autorités centrales chargées de l'entraide peuvent être sollicitées pour aider à se coordonner dans ces circonstances.

Paragraphe 5

212. Le paragraphe 5 prévoit que, si des mesures d'enquêtes doivent être prises sur le territoire de l'une des Parties participantes, les autorités participantes de cette dernière peuvent demander à leurs propres autorités d'effectuer lesdites mesures. Ces dernières déterminent en fonction de leur droit interne si elles le peuvent. Si elles sont en mesure de le faire, il n'est pas nécessaire que d'autres Parties participantes présentent une demande d'entraide. Cette disposition couvre l'un des aspects les plus innovants des ECE. Toutefois, dans certains cas, il est possible que ces autorités n'aient pas la compétence nécessaire en droit interne pour effectuer une mesure d'enquête pour le compte d'une autre Partie sans demande d'entraide.

Paragraphe 6

213. Le paragraphe 6 traite de l'utilisation des informations ou preuves communiquées aux autorités participantes d'une Partie par les autorités participantes d'une autre Partie. L'utilisation peut être refusée ou limitée conformément aux termes d'un accord tel que visé aux paragraphes 1 et 2; toutefois, si cet accord ne prévoit rien en termes de refus ou de limitation de l'utilisation, les informations ou preuves peuvent être utilisées selon les modalités prévues au paragraphe 6 a à c. Les circonstances prévues au paragraphe 6 s'appliquent sans préjudice des conditions fixées pour les transferts ultérieurs d'informations ou de preuves à un autre État telles que prévues à l'Article 14.

214. Il convient de noter que, lorsque les paragraphes 6.a à c s'appliquent, les autorités participantes peuvent néanmoins convenir entre elles de limiter davantage l'utilisation

d'informations ou preuves particulières pour éviter de nuire à l'une de leurs enquêtes, soit avant, soit après la fourniture des informations ou preuves. Ainsi, même si l'utilisation de preuves par la Partie qui les a reçues répond à l'un des objectifs pour lesquels l'ECE avait été établie, cela peut nuire à l'enquête de la Partie qui fournit les informations ou preuves (par exemple en révélant à un groupe criminel qu'une enquête est en train d'être menée sur eux, ce qui risque de les faire fuir, de les amener à détruire des preuves ou à intimider des témoins). Dans ce cas, la Partie qui a fourni les informations ou preuves peut demander à l'autre Partie d'accepter de ne pas les rendre publiques tant que le risque n'a pas disparu.

215. Au paragraphe 6.b, les rédacteurs visaient la situation où, en l'absence d'accord prévoyant les conditions du refus ou de la limitation de l'utilisation des informations ou preuves obtenues dans le cadre de l'ECE, il ne serait pas nécessaire d'obtenir le consentement des autorités les ayant fournies dans le cas où, en vertu des principes juridiques fondamentaux de la Partie dont les autorités participantes les ont reçues, ces informations ou preuves importantes pour une défense effective dans une procédure concernant d'autres infractions doivent être absolument divulguées à la défense ou à une autorité judiciaire. Même si, dans ce cas, le consentement n'est pas exigé, la divulgation des informations et preuves à cette fin sera notifiée sans retard indu. Si possible, elle devrait intervenir avant la divulgation, afin de permettre à la Partie qui a fourni les informations ou preuves de se préparer à leur divulgation et de mettre les Parties en mesure de se consulter en tant que de besoin.

216. Selon la compréhension des rédacteurs, le paragraphe 6.c fait référence à des circonstances exceptionnelles dans lesquelles les autorités de la Partie destinataire pourraient utiliser directement les informations ou preuves pour prévenir une urgence, telle que définie à l'Article 3, paragraphe 2.c de ce Protocole. La sécurité d'une personne physique signifie des dommages corporels graves. La notion de "risque significatif et imminent pour la vie ou la sécurité d'une personne" est expliquée plus en détail dans le Rapport explicatif au paragraphe 42 qui fournit aussi des exemples de ce type de situation. Les rédacteurs ont considéré que cette notion inclut les situations dans lesquelles un risque significatif et imminent pour des biens ou réseaux met en cause la vie ou la sécurité d'une personne physique. Si des informations ou preuves sont utilisées en application de l'alinéa 6.c, les autorités participantes de la Partie qui les a fournies doivent en être notifiées sans retard indu sauf autre accord. Ainsi, par exemple, les autorités participantes peuvent décider que l'autorité centrale devrait être notifiée.

Paragraphe 7

217. Enfin, il convient de rappeler de manière générale qu'il existe une longue histoire de coopération internationale mise en œuvre directement au cas par cas entre partenaires des services répressifs, dans le cadre de laquelle une équipe de procureurs et/ou enquêteurs d'un pays coopère avec ses homologues étrangers dans une enquête spécifique, selon un format autre que celui d'une ECE. Le paragraphe 7 couvre ces cas de coopération internationale et, pour les Parties qui en auraient besoin, fournit une base juridique internationale pour mener une enquête conjointe sans un accord tel que visé aux paragraphes 1 et 2. Comme pour toutes les mesures prévues par le présent protocole, les enquêtes conjointes visées au paragraphe 7 sont soumises aux conditions et garanties du chapitre III.

Chapitre III – Conditions et garanties

Article 13 – Conditions et garanties

218. Fondé sur l'article 15 de la Convention, l'article 13 prévoit que « chaque Partie veille à ce que l'établissement, la mise en œuvre et l'application des pouvoirs et procédures prévus par le présent Protocole soient soumis aux conditions et garanties prévues par son droit interne, qui assure une protection adéquate des droits de l'homme et des libertés ». Cet article étant fondé sur l'article 15 de la Convention, l'explication de cet article aux paragraphes 145 à 148 du Rapport explicatif de la Convention est également valable pour l'article 13 du présent Protocole, notamment le fait que le principe de proportionnalité « est mis en œuvre par chaque Partie conformément aux principes pertinents de son droit interne » (voir paragraphe 146 du Rapport explicatif de la Convention).

219. Il convient de noter qu'en plus de cet article, d'autres articles contiennent des garanties importantes. Par exemple, les mesures prévues par le présent Protocole ont un champ d'application limité, c'est-à-dire « aux enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des systèmes et des données informatiques, et à la collecte de preuves sous forme électronique d'une infraction pénale » (voir article 2). En outre, certains articles précisent les informations à inclure dans les demandes, les ordonnances et les informations d'accompagnement qui peuvent aider à appliquer les garanties nationales (voir l'article 7, paragraphes 3 et 4; l'article 6, paragraphe 3; l'article 8, paragraphe 3; l'article 9, paragraphe 3). En outre, les types de données à divulguer sont précisés dans chaque article, comme par exemple à l'article 7 qui est limité aux informations sur les abonnés. De plus, les Parties peuvent émettre des réserves et des déclarations, par exemple, pour limiter le type d'informations à fournir comme dans les articles 7 et 8. Enfin, lorsque des données à caractère personnel sont transférées en vertu du présent Protocole, les garanties de protection des données de l'article 14 s'appliquent.

Article 14 – Protection des données à caractère personnel

Paragraphe 1 – Champ d'application

220. Les mesures prévues au chapitre II du présent Protocole nécessitent souvent le transfert de données à caractère personnel. Étant donné qu'un grand nombre de Parties au Protocole peuvent être tenues, pour se conformer à leurs obligations constitutionnelles ou internationales, d'assurer la protection des données à caractères personnel, l'article 14 prévoit des garanties de protection des données à caractère personnel pour permettre aux Parties de satisfaire à ces obligations et de rendre ainsi possible le traitement de données à caractère personnel aux fins du présent Protocole.

221. En vertu du paragraphe 1.a, chaque Partie est tenue de traiter les données à caractère personnels qu'elle reçoit en vertu du présent Protocole conformément aux garanties expressément prévues aux paragraphes 2 à 15. Sont également couvertes les données à caractère personnel transférées en exécution d'une injonction ou d'une demande faite en vertu du présent Protocole. Toutefois, les paragraphes 2 à 15 ne s'appliquent pas si les conditions des exceptions exposées aux paragraphes 1.b ou 1.c sont applicables.

222. La première exception figure au paragraphe 1.b, qui dispose que « [s]i, au moment de la réception de données à caractère personnel en vertu du présent Protocole, la Partie de transfert et la Partie destinataire sont toutes deux liées par un accord international établissant un cadre global entre ces Parties pour la protection des données à caractère personnel, applicable au transfert de données à caractère personnel aux fins de la prévention, de la détection, de l'investigation et de la poursuite d'infractions pénales, et qui prévoit que le traitement des données à caractère personnel en vertu de cet accord est conforme aux exigences de la législation sur la protection des données des Parties concernées, les termes de cet accord s'appliquent, pour les mesures relevant du champ d'application du présent Protocole, aux données à caractère personnel reçues en vertu du Protocole

en lieu et place des paragraphes 2 à 15, sauf accord contraire entre les Parties concernées. » À cet égard, un cadre serait généralement considéré comme « global » s'il couvre l'ensemble des aspects de la protection des données pour les transferts de données. Deux exemples d'accords visés au paragraphe 1.b sont la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) telle que modifiée par son Protocole d'amendement (STCE n° 223) et l'Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. Les termes de ces accords s'appliquent en lieu et place des paragraphes 2 à 15 en ce qui concerne les mesures entrant dans leur champ d'application. Pour les Parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) telle que modifiée par son Protocole d'amendement (STCE n° 223), il en résulte que l'article 14, paragraphe 1, tel qu'expliqué en détail aux paragraphes 105 à 107 du Rapport explicatif au Protocole d'amendement, est applicable. En termes de chronologie, les paragraphes 2 à 15 de cet article ne seront subrogés que si les Parties sont mutuellement liées par l'accord au moment de la réception de données à caractère personnel en vertu du présent Protocole. Cela vaut aussi longtemps que l'accord dispose que les données transférées en application de ses dispositions continueront d'être traitées dans les conditions qu'il définit.

223. La seconde exception est exposée au paragraphe 1.c, qui dispose que même si la Partie transférante et la Partie destinataire ne sont pas mutuellement liées par un accord du type de celui décrit au paragraphe 1.b, elles peuvent néanmoins déterminer conjointement que le transfert de données à caractère personnel en vertu du présent Protocole peut se faire sur la base d'autres accords ou arrangements en lieu et place des paragraphes 2 à 15 de cet article. Ceci garantit aux Parties une certaine souplesse pour fixer les garanties de protection des données qui s'appliquent aux transferts effectués entre elles en vertu du présent Protocole. Dans un souci de sécurité juridique et de transparence pour les individus et pour les fournisseurs et les entités impliqués dans les transferts de données en application des mesures prévues à la section 2 du chapitre II de ce Protocole, les Parties sont encouragées à communiquer clairement au public leur détermination commune à ce qu'un accord ou un arrangement de cette nature régisse les aspects relatifs à la protection des données lors des transferts de données entre elles.

224. Les rédacteurs ont considéré que le Protocole garantit des protections satisfaisantes pour les transferts de données effectués en application de ses dispositions grâce aux garanties de protection des données prévues aux paragraphes 2 à 15. À cette fin, conformément au paragraphe 1.d, les transferts de données visés au paragraphe 1.a seront réputés satisfaire aux exigences du cadre juridique de chacune des Parties régissant la protection des données pour les transferts internationaux de données à caractère personnel ; en conséquence, aucune autre autorisation ne sera requise en vertu de ces cadres juridiques pour ces transferts. En outre, dans la mesure où les dispositions des accords décrits au paragraphe 1.b établissent que le traitement des données à caractère personnel en vertu de ces accords satisfait aux exigences de la législation des Parties concernées relative à la protection des données, le paragraphe 1.d étend cette approbation aux transferts effectués en vertu du présent Protocole. Ce paragraphe est donc producteur de sécurité juridique pour les transferts internationaux de données à caractère personnel effectués en vertu des paragraphes 1.a ou 1.b en réponse aux injonctions ou demandes adressées en vertu du présent Protocole, le but étant de garantir l'efficacité et la prévisibilité des échanges de données. Comme les accords ou arrangements décrits au paragraphe 1.c ne font pas nécessairement mention de la conformité au cadre juridique des Parties relatif à la protection des données – par exemple dans le cas des traités bilatéraux d'entraide judiciaire –, ils ne reçoivent pas la même approbation en vertu de ce Protocole que dans les cas relevant des paragraphes 1.a ou 1.b. Toutefois, les Parties concernées peuvent décider d'un commun accord que cette approbation est acquise.

225. De plus, le paragraphe 1.d dispose qu'une Partie est autorisée à refuser ou à empêcher les transferts de données à une autre Partie en vertu du présent Protocole uniquement pour des raisons de protection des données : (i) dans les conditions exposées au paragraphe 15 relatif à la

consultation et à la suspension ou (ii) aux termes d'accords ou d'arrangements spécifiques visés aux paragraphes 1.b ou 1.c, lorsque l'un de ces paragraphes s'applique.

226. Enfin, l'objectif de cet article est d'établir des garanties satisfaisantes pour permettre le transfert de données à caractère personnel entre les Parties au présent Protocole. L'article 14 n'impose pas une harmonisation des cadres juridiques nationaux régissant le traitement général des données à caractère personnel ni du cadre relatif au traitement spécifique des données à caractère personnel aux fins de l'application du droit pénal. Le paragraphe 1.e dispose que rien n'empêche les Parties d'appliquer des garanties plus strictes que celles prévues aux paragraphes 2 à 15 pour le traitement, par leurs autorités respectives, des données à caractère personnel reçues en vertu du présent Protocole. Inversement, le paragraphe 1.e. n'a pas pour but de permettre aux Parties d'imposer des conditions supplémentaires de protection des données autres que celles expressément prévues dans cet article pour les transferts de données effectués en vertu du présent Protocole.

Paragraphe 2 – But et utilisation

227. Le paragraphe 2 traite des buts et de l'utilisation pour lesquels les Parties peuvent procéder au traitement de données à caractère personnel en vertu du présent Protocole. Le paragraphe 2.a dispose que « la Partie destinataire de données personnelles (« Partie destinataire ») traite les données aux fins prévues à l'article 2 », c'est-à-dire aux fins « [d']enquêtes ou procédures pénales spécifiques concernant des infractions pénales liées à des données et systèmes informatiques » et de « recueil de preuves d'une infraction pénale sous forme électronique » et, pour ce qui concerne les Parties au Premier Protocole, aux fins « d'enquêtes ou procédures pénales spécifiques concernant les infractions pénales établies dans le Premier Protocole ». En d'autres termes, il faut que les autorités aient ouvert une enquête ou entamé des poursuites concernant une activité criminelle définie, cette enquête ou ces poursuites constituant le but légitime dans lequel il est possible de rechercher des preuves ou des informations contenant des données à caractère personnel et de les traiter.

228. Si la raison première pour laquelle le Protocole peut être invoqué est uniquement l'obtention d'informations ou de preuves dans une enquête ou une procédure pénale donnée, à l'exclusion d'autres fins, le paragraphe 2.a dispose aussi qu'une Partie « ne [doit pas procéder] à d'autres traitements des données personnelles dans un but incompatible avec l'article 2 et [qu']elle ne traite pas non plus les données lorsque son cadre juridique ne l'autorise pas ». Pour déterminer si la finalité d'un traitement supplémentaire n'est pas incompatible avec le but initial, l'autorité compétente est encouragée à procéder à une évaluation globale des circonstances de l'espèce comme (i) le rapport entre le but initial et le but supplémentaire ultérieur (établi par un éventuel lien objectif, par exemple) ; (ii) les conséquences (potentielles) pour les personnes concernées de l'utilisation supplémentaire envisagée, en tenant compte de la nature des données à caractère personnel (leur sensibilité, par exemple) ; (iii) les attentes raisonnables potentielles des personnes concernées quant au but de cette utilisation supplémentaire et à l'égard des entités qui pourraient traiter les données, et (iv) la manière dont les données seront traitées et protégées contre toute utilisation indue. Le cadre juridique d'une Partie peut fixer des limites particulières concernant d'autres objectifs pour lesquels les données peuvent être utilisées.

229. Le traitement des données dans un but qui ne soit pas incompatible devrait normalement comprendre leur utilisation à des fins de coopération internationale conformément aux législations nationales et aux accords ou arrangements internationaux en matière pénale (pour l'entraide judiciaire, par exemple). Il pourrait aussi inclure, entre autres, des utilisations dans le cadre de certaines fonctions administratives, comme les déclarations aux organes de contrôle, les enquêtes connexes sur des infractions au droit pénal, civil ou administratif (y compris les enquêtes menées par d'autres instances administratives) et leur jugement, les divulgations ordonnées par décision de justice, la divulgation à des personnes privées parties à un litige, la communication de certaines informations à l'avocat d'un accusé et la divulgation directe au public ou aux médias (y compris dans

le cadre des demandes d'accès aux documents et de procédures judiciaires publiques). De même, un traitement supplémentaire des données à caractère personnel à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique, ou à des fins statistiques pourrait être considéré comme compatible avec l'article 2.

230. Le paragraphe 2.a autorise en outre les Parties à imposer des conditions et restrictions supplémentaires à l'utilisation de données à caractère personnel dans des cas donnés, dans la mesure prévue au chapitre II du présent Protocole. Toutefois, ces conditions ne doivent pas comporter de conditions génériques de protection des données – c'est-à-dire des conditions qui ne soient pas propres à des cas donnés – allant au-delà de celles prévues par cert article. À titre d'exemple, différents systèmes de supervision sont admis en vertu de l'article 14 et une Partie n'est pas autorisée à poser comme condition préalable au transfert de données dans un cas individuel que la Partie requérante dispose de l'équivalent d'une autorisée spécialisée de protection des données.

231. Enfin, le paragraphe 2.b fait obligation à la Partie destinataire, lorsqu'elle cherche à obtenir des données à caractère personnel et les utilise en vertu du présent Protocole, « [de veiller], dans le cadre de son droit interne, à ce que les données à caractère personnel demandées et traitées soient pertinentes et qu'elles ne soient pas excessives au regard de la finalité de ce traitement ». Cette obligation peut par exemple être mise en œuvre au moyen des règles de la preuve et de limitations de la portée des injonctions contraignantes, des principes de nécessité, de proportionnalité et du caractère raisonnable, et de directives et politiques internes limitant la collecte ou l'utilisation des données. Les Parties sont également encouragées à considérer, dans leurs cadres juridiques nationaux, les situations impliquant des personnes vulnérables, comme les victimes ou les mineurs, par exemple.

Paragraphe 3 – Qualité et intégrité

232. Le paragraphe 3 impose aux Parties de prendre « des mesures raisonnables pour veiller à ce que les données à caractère personnel soient conservées de manière aussi exacte et complète et soient aussi actuelles qu'il est nécessaire et approprié pour qu'elles puissent être traitées conformément à la loi compte tenu des buts dans lesquels elles sont traitées. ». Le contexte est important et ce principe peut donc être mis en œuvre différemment selon les situations. Il ne s'appliquerait par exemple pas de la même manière à des fins de poursuites pénales que dans d'autres buts.

233. S'agissant des enquêtes et des procédures pénales, le paragraphe 3 ne doit pas être interprété dans le sens qu'il imposerait aux autorités de poursuites pénales de modifier les informations qui pourraient servir de preuves dans une affaire pénale – même lorsque ces informations sont inexactes ou incomplètes –, parce que l'inexactitude de ces données peut être un élément majeur de l'infraction (par exemple en cas de fraude) et parce que cela saperait en outre l'objectif d'équité à l'égard de l'accusé si les autorités modifiaient une preuve recueillie grâce au présent Protocole.

234. Dans de nombreuses situations, lorsqu'il y a des doutes quant à la fiabilité des données à caractère personnel, cela devrait être clairement indiqué. Par exemple, dans la mesure où des informations ou des preuves ont été reçues grâce au présent Protocole sont utilisées pour retracer une conduite criminelle passée, les procédures applicables devraient prévoir les moyens de corriger ou de garder la trace des erreurs dans les informations (notamment en modifiant ou en complétant les informations originales) et d'actualiser, modifier ou compléter les données peu fiables ou obsolètes afin de minimiser le risque que les autorités prennent des mesures répressives inappropriées ou potentiellement défavorables sur la base de données de mauvaise qualité (par exemple en arrêtant la mauvaise personne ou en arrêtant une personne en s'appuyant sur une compréhension erronée de son comportement). Les Parties sont encouragées à prendre des mesures raisonnables pour s'assurer que lorsque des données communiquées à une autre autorité ou reçues

d'une autre autorité se révèlent inexactes ou obsolètes, cette autre autorité en est informée aussi rapidement que possible afin qu'il puisse être procédé aux corrections nécessaires et appropriées compte tenu des finalités du traitement.

Paragraphe 4 – Données sensibles

235. Le paragraphe 4 concerne les mesures qui doivent être prises par les Parties en vertu du présent Protocole lorsqu'elles traitent certains types de données qui peuvent être nécessaires, en particulier, à titre de preuves dans une enquête ou une procédure pénale mais dont la nature impose que des garanties appropriées soient prises pour se prémunir contre le risque d'effets préjudiciables injustifiés pour la personne concernée par l'utilisation de ces données, en particulier contre le risque de discrimination illicite.

236. Aux termes du paragraphe 4, les données sensibles sont notamment « les données à caractère personnel révélant l'origine ethnique ou raciale, les opinions politiques, les croyances religieuses ou autres, ou l'affiliation syndicale, ainsi que [les] données génétiques, [les]données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent ou [les] données à caractère personnel concernant la santé ou la sexualité », ce dernier élément recouvrant à la fois l'orientation sexuelle et les pratiques sexuelles. Les données relatives à la santé peuvent comprendre des données relatives à la santé physique ou mentale d'une personne qui révèlent des informations sur son état de santé passé, présent ou futur (comme des informations sur une maladie, un handicap, un risque de maladie, l'historique médical d'une personne ou ses traitements, ou encore son état physiologique ou biomédical). Les données génétiques peuvent comprendre, par exemple, les résultats d'analyses chromosomiques, d'ADN ou d'ARN, qui concernent les caractéristiques génétiques héritées ou acquises d'une personne et contiennent des informations uniques sur sa physiologie, sa santé ou sa filiation.

237. La notion de données biométriques couvre toute une série d'identifiants uniques résultant de caractéristiques physiques ou physiologiques mesurables utilisées pour identifier une personne ou vérifier l'identité déclinée par cette dernière (empreintes digitales, motif de l'iris ou des veines de la main, schémas vocaux, photographies ou séquences vidéo, par exemple). Certaines Parties considèrent aussi que les identifiants uniques fournis par des caractéristiques biologiques ou comportementales constituent des données biométriques. Si certaines formes de données biométriques peuvent être jugées sensibles au vu des risques qu'elles impliquent, ce n'est pas le cas de toutes. Ainsi, certaines Parties considèrent que les données biométriques qui sont informatisées ou extraites d'un échantillon ou d'une image biométrique (comme les modèles biométriques) sont des données sensibles. Inversement, certaines photographies ou séquences vidéo, même si elles révèlent des caractéristiques physiques ou anatomiques telles que des cicatrices, des marques sur la peau et des tatouages, ne seront généralement pas considérées comme des données biométriques sensibles. Puisque le niveau de sensibilité des données biométriques peut varier, le paragraphe 4 offre aux Parties une latitude pour réglementer cette question en indiquant que les données sensibles comprennent les « données biométriques considérées comme sensibles compte tenu des risques qu'elles comportent ». Cette formulation reconnaît que la biométrie est un domaine en évolution et que les données considérées comme « sensibles » aux termes de ce paragraphe devront faire l'objet d'une évaluation dans la durée au regard des nouveautés technologiques et en matière de techniques d'enquête et autres et compte tenu des risques qu'elles entraînent pour les personnes concernées. En ce qui concerne les Parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), telle qu'amendée par le Protocole (STCE n° 223), l'interprétation de ce qui constitue des données biométriques "sensibles" devrait être guidée par l'article 6, paragraphe 1, de cette Convention, tel que détaillé aux paragraphes 58 et 59 du Rapport explicatif de cette Convention.

238. L'utilisation abusive et le traitement indu de données sensibles présentent des risques de préjudice pour les personnes concernées, notamment des risques de discrimination illicite. Le

système de justice pénale devrait être configuré de sorte à assurer une protection contre les conséquences préjudiciables injustifiées et la discrimination illicite fondée, par exemple, sur l'utilisation de preuves révélant la race, la religion ou la sexualité d'une personne. Pour donner un autre exemple, ce paragraphe reconnaît aussi l'importance de protéger contre le risque de préjudice causé par la divulgation injustifiée ou illégale afin d'éviter, par exemple, qu'une personne soit ostracisée en raison d'informations révélant son orientation sexuelle ou son identité de genre. À cet égard, le paragraphe 4 exige des Parties qu'elles mettent en place des « garanties appropriées » pour se prémunir contre ces risques.

239. Le caractère approprié des garanties devrait être apprécié au regard de la sensibilité des données, de la portée, du contexte, des buts et de la nature du traitement (par exemple en cas de prise de décisions automatisée) ainsi que de la probabilité et de la gravité des risques. Ces garanties peuvent varier d'un système juridique interne à l'autre et dépendre de ces facteurs. Une liste non exhaustive de garanties pourrait inclure la restriction du traitement des données (qui ne serait, par exemple, autorisé qu'au cas par cas ou à certaines fins), la limitation de leur diffusion, la restriction de l'accès à ces dernières (ouvert seulement à certains personnels, par exemple, en vertu de procédures spéciales d'autorisation ou d'authentification nécessitant une formation spécialisée de ces personnels), des mesures organisationnelles ou techniques de sécurité supplémentaires (comme le masquage, la pseudonymisation ou le stockage séparé des données biométriques et des informations biographiques correspondantes) ou des durées de conservation plus courtes. Dans certains cas, il peut être utile de procéder à une analyse d'impact pour faciliter l'identification et la gestion des risques.

Paragraphe 5 – Périodes de conservation

240. La première phrase du paragraphe 5 dispose que « [c]haque Partie conserve les données à caractère personnel uniquement pour la durée nécessaire et appropriée aux fins du traitement des données prévu au paragraphe 2 ». À cet égard, le principe de limitation des buts énoncé au paragraphe 2 dispose qu'une Partie destinataire de données à caractère personnel doit les traiter dans des buts définis conformément à l'article 2 et ne doit pas les soumettre à d'autres traitements dans un but incompatible avec cet article. Conformément à ce principe, la durée de conservation des données dépend des buts définis dans lesquels ces données sont traitées.

241. En vertu de l'article 2, les données à caractère personnel reçues par une Partie en vertu du présent Protocole l'étant à des fins d'enquêtes ou de procédures pénales spécifiques, ces données peuvent être conservées aussi longtemps que nécessaire (a) pendant la durée de l'enquête et de la procédure subséquente, y compris les éventuelles procédures en appel ou la durée au cours de laquelle une affaire peut être rouverte en vertu du droit interne et (b) pour faire l'objet d'un traitement supplémentaire dans un but qui n'est « pas incompatible » avec le but premier de la collecte après que celui-ci a été atteint. Ainsi, une Partie peut disposer que les informations ou preuves soient conservées à des fins d'archivage ou de recherches historiques, ou d'autres buts compatibles, conformément à l'article 14, paragraphe 2, comme exposé plus en détail dans les paragraphes correspondants du présent Rapport explicatif.

242. La deuxième phrase du paragraphe 5 offre aux Parties deux possibilités pour satisfaire à l'obligation de ne pas conserver des données à caractère personnel plus longtemps que nécessaire et approprié au vu des finalités de leur traitement en vertu du paragraphe 2 de cet article. Premièrement, une Partie peut fixer des durées de conservation déterminées dans son droit interne. Sinon, les Parties peuvent prévoir dans leur droit interne que la nécessité de conserver plus longtemps les données soit revue à intervalles programmés. Les Parties disposent d'une marge discrétionnaire pour décider de l'approche la plus adaptée aux données concernées en l'espèce dans le contexte de leur cadre juridique interne. Les Parties peuvent aussi prévoir une durée de conservation déterminée assortie d'un système de révision périodique à intervalles plus courts. Elles devraient garantir dans leur cadre juridique que les autorités compétentes élaborent des règles et/ou procédures internes pour la mise en œuvre des durées de conservation déterminées et/ou des

révisions périodiques de la nécessité de prolonger la conservation. Lorsque la durée de conservation est écoulée ou lorsque la Partie a établi, dans le cadre de la révision périodique, qu'il n'est plus nécessaire de conserver les données, celles-ci doivent être supprimées ou anonymisées.

Paragraphe 6 – Décisions automatisées

243. Le paragraphe 6 concerne la protection des personnes lorsque des décisions emportant des conséquences négatives importantes pour les intérêts en jeu pour elles sont basées uniquement sur le traitement automatisé de leurs données personnelles. Il ne devrait pas arriver fréquemment que des décisions soient prises de façon automatisée lorsqu'une Partie sera destinataire de données à caractère personnel provenant d'une autre Partie en vertu du présent Protocole car les preuves ou les informations seront recueillies par des enquêteurs ou des autorités judiciaires aux fins d'une enquête ou d'une procédure pénale déterminée. Néanmoins, lorsque la prise de décisions ayant un effet défavorable significatif sur les intérêts en jeu pour la personne à laquelle se rapportent les données à caractère personnel se fait de manière automatisée dans le cadre de l'enquête pour laquelle ces données ont été demandées, les autorités doivent appliquer cette disposition. Elle doivent aussi l'appliquer lorsque les données sont utilisées par la suite à des fins de prévention, de détection, d'enquête ou de poursuites relatives à d'autres infractions (arrestation basée sur le traitement purement automatisé de profils criminels, de données relatives aux condamnations, aux libérations conditionnelles et sous caution, par exemple) ou dans un but compatible (par exemple dans le cadre de la vérification des antécédents), si les données font l'objet d'un traitement par des outils d'analyse automatisée pour la prise de décisions.

244. Par conséquent, le paragraphe 6 interdit les décisions basées exclusivement sur le traitement automatisé de données à caractère personnel lorsque ces décisions ont des répercussions négatives importantes sur les intérêts en jeu pour la personne concernée, y compris sur le plan juridique (en raison des incidences sur la situation juridique ou les droits de l'intéressé), comme l'émission d'un mandat d'arrêt ou le refus d'une libération conditionnelle ou sous caution, à moins que cette prise de décisions automatisée soit autorisée en droit interne et s'accompagne de garanties appropriées.

245. Des garanties appropriées sont essentielles pour réduire l'impact potentiel sur les intérêts en jeu pour la personne à laquelle les données à caractère personnel se rapportent. Ces garanties devraient comprendre la possibilité pour la personne concernée d'obtenir une intervention humaine pour évaluer la décision. Les Parties sont également encouragées à prendre des mesures raisonnables pour assurer la qualité et la représentativité des données utilisées pour développer les algorithmes ainsi que l'exactitude des inférences statistiques utilisées en tenant compte des circonstances et du contexte spécifiques, y compris le contexte pénal.

Paragraphe 7 – Sécurité des données et incidents de sécurité

246. En vertu du paragraphe 7.a, « [c]haque Partie s'assure de disposer de mesures technologiques, physiques et organisationnelles appropriées pour la protection des données à caractère personnel ». Par exemple, ces mesures technologiques peuvent inclure des logiciels de protection contre les logiciels malveillants, le cryptage des données et des pares-feux. Les mesures physiques peuvent comprendre l'hébergement des serveurs et fichiers informatiques dans des lieux sécurisés et les mesures organisationnelles peuvent consister en diverses règles, pratiques, politiques et procédures, visant notamment à limiter les droits d'accès.

247. Le paragraphe 7.a dispose en outre que ces mesures doivent protéger en particulier contre la perte (par exemple au moyen de procédures standardisées pour l'enregistrement et le maniement des données), contre l'accès accidentel ou non autorisé (par exemple au moyen de protections contre les intrusions informatiques, de conditions d'autorisation ou d'authentification pour l'accès aux dossiers papier ou aux fichiers informatiques), contre la divulgation accidentelle ou non autorisée (par exemple au moyen de mesures technologiques de détection et de prévention des

divulgations accidentelles ou non autorisées et de mesures organisationnelles pour indiquer les conséquences de telles divulgations) et contre l'altération ou la destructions accidentelle ou non autorisée de données (par exemple en restreignant la saisie ou la modification de données électroniques ou de dossiers papier au personnel autorisé, en utilisant des systèmes d'enregistrement, en affichant les durées de conservation ou en installant des systèmes de sauvegarde des fichiers informatiques et des dossiers papier).

248. Les modalités précises arrêtées pour satisfaire à ces obligations, d'une manière adaptée aux circonstances particulières de l'espèce, sont laissées à la discrétion de la Partie concernée. Les Parties sont par exemple encouragées à concevoir et mettre en œuvre des mesures de sécurité qui prennent en compte des facteurs tels que la nature des données à caractère personnel (notamment leur sensibilité), les risques identifiés et les conséquences négatives potentielles pour la personne concernée en cas d'incident de sécurité. Les Parties peuvent aussi prendre en compte la question des ressources nécessaires pour la conception et l'application des mesures de sécurité des données. Elles sont encouragées à revoir périodiquement ces mesures et à les actualiser si nécessaire au vu de l'évolution de la technologie et de la nature des risques.

249. Le paragraphe 7.b expose les obligations en cas d'incident de sécurité (tel que défini au paragraphe 7.a et décrit ci-dessus) concernant les données à caractère personnel reçues en vertu du présent Protocole et créant un « risque significatif de préjudice matériel ou non matériel » aux personnes ou à la Partie de laquelle proviennent les données. Les préjudices aux personnes visés ici sont notamment les préjudices corporels ou de réputation, la détresse émotionnelle (par exemple en raison de l'humiliation ou d'une violation de la confidentialité), la discrimination ou les préjudices financiers (par exemple en raison de la perte de l'emploi ou d'opportunités professionnelles, d'une note de la qualité de crédit négative, de l'usurpation d'identité ou du risque de chantage). Pour l'autre Partie, le risque peut en particulier résider dans l'impact négatif potentiel sur une enquête parallèle (par exemple avec la fuite du suspect ou la destruction de preuves). S'il y a un « risque significatif » que de tels préjudices surviennent, la Partie destinataire a l'obligation « [d'évaluer] sans tarder la probabilité de survenance et l'importance » du préjudice et de « prend[re] rapidement les mesures appropriées pour atténuer ce préjudice ». Les facteurs relatifs à la probabilité et à l'importance du préjudice à prendre en considération sont, entre autres, le type d'incident, comme le fait, s'il est connu, qu'il repose sur une intention de nuire et l'identité des personnes en possession des informations ou qui ont pu les obtenir, la nature et la sensibilité des données concernées, le volume de données potentiellement compromises et le nombre de personnes potentiellement touchées, la possibilité d'identifier facilement les personnes concernées, la probabilité qu'il y ait eu accès aux données et qu'elles aient été utilisées, selon qu'elles aient été cryptées, par exemple, ou rendues inaccessibles d'une autre manière, ainsi que les conséquences qui pourraient résulter de cet incident.

250. Conformément aux mesures décrites au paragraphe 7.a et afin d'apporter la réponse appropriée visée au paragraphe 7.b, les Parties sont tenues de disposer de procédures internes permettant de détecter les incidents de sécurité. Elles devraient également disposer d'une procédure leur permettant d'évaluer rapidement la probabilité de survenance d'une préjudice potentiel et son ampleur et de prendre rapidement les mesures appropriées pour le limiter (par exemple en demandant le retour ou la suppression des données transmises accidentellement à un destinataire non autorisé). L'application effective de ces obligations peut être facilitée par l'existence de procédures internes de signalement et par la consignation de tous les incidents de sécurité.

251. Le paragraphe 7.b énumère aussi les circonstances dans lesquelles l'autre Partie et les personnes concernées doivent recevoir notification de l'incident, sous réserve des exceptions et restrictions prévues à cette obligation de notification.

252. En cas d'incident de sécurité comportant un risque significatif de préjudice matériel ou non matériel à des personnes ou à l'autre Partie, notification doit en être faite à l'autorité transférante ou, aux fins de la section 2 du chapitre II, à l'autorité ou aux autorités désignées conformément au

paragraphe 7.c. Toutefois, cette notification peut être assortie de restrictions appropriées quant à la transmission de cette notification à des tiers ; elle peut être différée ou omise lorsqu'elle risque de porter atteinte à la sécurité nationale ou être différée lorsqu'elle risque de compromettre des mesures visant à protéger la sécurité publique (y compris lorsqu'elle compromettrait l'enquête sur les infractions pénales découlant de l'incident de sécurité). Pour décider s'il convient de différer ou d'omettre la notification dans des circonstances où celle-ci pourrait mettre en danger la sécurité nationale, une Partie devrait se demander s'il est raisonnable, dans ces circonstances, d'omettre la notification ou s'il ne serait pas plus approprié de la différer.

253. En cas d'incident de sécurité comportant un risque important de préjudice matériel ou non matériel à des personnes, les personnes concernées par cet incident doivent également en recevoir notification afin de pouvoir protéger leurs intérêts, cette obligation de notification étant toutefois soumise à des exceptions. Premièrement, le paragraphe 7.b indique qu'il n'est pas nécessaire de procéder à cette notification si la Partie a pris des mesures appropriées de sorte qu'il n'y a plus de risque significatif de préjudice. Par exemple, aucune notification ne serait nécessaire lorsqu'un e-mail contenant des informations personnelles sensibles a été envoyé par mégarde au mauvais destinataire, ce qui aurait constitué un risque significatif de préjudice sans mesures d'atténuation de ce risque, mais que le destinataire a, sur demande, rapidement et définitivement supprimé ce message sans qu'il soit diffusé plus largement. Deuxièmement, la notification à une personne peut être omise ou différée dans les conditions prévues au paragraphe 12.a.i – à savoir que la notification « [peut être soumise] à l'application de restrictions proportionnées autorisées par son cadre juridique interne, nécessaires […] pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et qui tiennent dûment compte des intérêts légitimes de la personne concernée ».

254. De manière générale, les Parties sont encouragées à inclure dans cette notification en vertu du paragraphe 7.b, et s'il y a lieu, des informations sur le type d'incident de sécurité, la nature et le volume des informations potentiellement compromises, les risques possibles et les mesures envisagées pour limiter les préjudices éventuels, y compris les mesures visant à contenir l'incident. Étant donné la fonction de supervision exercée par les autorités de supervision décrites au paragraphe 14 et afin de bénéficier de conseils d'experts pour la gestion de l'incident, il pourrait également être utile que la Partie qui émet la notification informe ces autorités de l'incident et des mesures d'atténuation prises le cas échéant.

255. Pour permettre une réponse coordonnée et y contribuer dans le cadre de ses propres mesures d'atténuation du risque, la Partie destinataire de la notification peut demander des consultations et des informations supplémentaires au sujet de l'incident et des mesures prises par la Partie émettrice de la notification pour y remédier.

256. Le paragraphe 7.c établit la procédure requise pour la désignation par les Parties de l'autorité ou des autorités auxquelles notification doit être faite en vertu du paragraphe 7.b aux fins du chapitre II, section 2.

Paragraphe 8 – Tenue des registres

257. Le paragraphe 8 impose aux Parties de « [tenir] des registres ou se dote[r] d'autres moyens appropriés pour montrer comment il est accédé aux données personnelles d'un individu, et comment celles-ci sont utilisées et divulguées dans un cas spécifique ». L'objectif est que chaque Partie dispose de moyens effectifs pour démontrer de quelle manière il a été accédé aux données à caractère personnel d'une personne et comment ces données ont été utilisées et divulguées dans ce cas précis, conformément au présent article. Il est important, en particulier à des fins de contrôle, de montrer que les règles ont été respectées, ce qui contribue en soi à la transparence et à la responsabilité. Si les moyens à mettre en œuvre pour montrer comment sont traitées les données sont laissés à la discrétion de chaque Partie, les Parties sont encouragées à adapter leurs méthodes

aux circonstances, en tenant compte des risques pour les personnes concernées et de la nature, de l'étendue, des finalités et du contexte global de ce traitement.

258. Certaines Parties peuvent, par exemple, décider d'utiliser l'enregistrement automatisé des activités (journal ou log) ou d'autres solutions (comme la consignation manuelle dans le cas de dossiers papier). Comme indiqué ci-dessus, l'objectif est de favoriser la transparence et la responsabilité tout en permettant une certaine souplesse quant à la manière dont une Partie remplit cet objectif, dans le respect des autres obligations applicables en vertu du présent article. Ainsi, les Parties devraient tenir des registres ou disposer d'autres documents relatifs à l'accès aux données, à leur utilisation ou à leur divulgation sous une forme qui facilite le travail des autorités de supervision.

Paragraphe 9 – Partage ultérieur au sein d'une Partie

259. Le paragraphe 9 dispose que « [l]orsqu'une autorité d'une Partie fournit des données à caractère personnel reçues initialement en vertu du présent Protocole à une autre autorité de cette Partie, cette dernière les traite conformément au présent article, sous réserve du paragraphe 9.b ». En d'autres termes, lorsque des données à caractère personnel reçues en vertu du présent Protocole sont ensuite communiquées à une autre autorité de la même Partie – y compris à une autorité d'un État constituant ou d'une autre entité territoriale similaire –, ces données doivent être traitées conformément au présent article, à moins que l'exception prévue au paragraphe 9.b s'applique. Le paragraphe 9 s'applique aussi en cas de partage ultérieur multiple.

260. Le paragraphe 9.b prévoit une exception au paragraphe 9.a dans le cas où un État fédéral partie au présent Protocole émet une réserve portant sur les obligations visées à l'article 17 du Protocole, conformément aux conditions fixées par cet article. En accord avec le paragraphe 298 du Rapport explicatif, cette exception a pour but de prendre en compte « les difficultés que des États fédéraux risquent de rencontrer en raison de la répartition typique des pouvoirs entre les autorités fédérales et régionales », qui correspond au paragraphe 316 du Rapport explicatif de la Convention. Par conséquent, le paragraphe 9.b dispose qu'une Partie qui a émis une réserve au titre de l'article 17 conserve la possibilité de communiquer des données à caractère personnel reçues en vertu du présent Protocole à ses États constituants ou autres entités territoriales similaires à condition qu'elle ait mis en place des mesures afin que les autorités destinataires continuent de protéger efficacement ces données en assurant un niveau de protection des données comparable à celui offert par le présent article. Une partie qui n'aurait pas « mis en place des mesures pour que les autorités qui reçoivent les données continuent à les protéger efficacement en assurant un niveau de protection des données comparable à celui offert par le présent article » se trouverait, en fonction de la gravité, des raisons et des circonstances du manquement à cette obligation, en situation de violation flagrante ou systématique du paragraphe 15 du présent article.

261. Le paragraphe 9.c prévoit que la Partie transférante est fondée, en cas d'indications selon lesquelles le présent paragraphe ne serait pas correctement appliqué par une autre Partie, à demander une consultation à cette autre Partie et des informations pertinentes sur ces indications afin de clarifier la situation.

Paragraphe 10 – Transfert ultérieur vers un autre État ou vers une organisation internationale

262. Aux termes du paragraphe 10.a, une Partie n'est autorisée à transférer des données à caractère personnel reçues en vertu du présent Protocole « à un autre État ou à une organisation internationale qu'avec l'autorisation préalable de l'autorité qui les lui a communiquées ou, aux fins de la section 2 du chapitre II, de l'autorité ou des autorités décrites au paragraphe 10.b ». Ce type de mesure conservatoire est une condition courante encadrant les transferts et dont le but est d'assister les partenaires étrangers dans le contexte de l'application du droit pénal (par exemple en vertu de traités d'entraide judiciaire ou de la coopération entre polices) ; cette approche est reprise

dans le présent paragraphe également comme un moyen de protéger les données à caractère personnel transférées en vertu du présent Protocole.

263. Le paragraphe 10.b dispose que chaque Partie doit, au moment de la signature ou lors du dépôt de son instrument de ratification, d'acceptation ou d'approbation, indiquer au Secrétaire Général du Conseil de l'Europe quelles sont l'autorité ou les autorités désignées pour donner l'autorisation visée au paragraphe 10.a aux fins des transferts en vertu de la section 2 du chapitre II ; les autorités ainsi désignées peuvent être modifiées par la suite.

264. L'obtention d'une autorisation de transfert ultérieur peut nécessiter l'envoi d'une demande individualisée par les autorités de la Partie destinataire en vue du transfert de données à caractère personnel spécifiées à un pays tiers ou à une organisation internationale donnée. Toutefois, le paragraphe 10.a n'empêche pas les Parties de fixer à l'avance les règles régissant les transferts ultérieurs (par exemple par voie d'un accord écrit ou selon d'autres modalités). Le paragraphe 10.a ne fait pas non plus obstacle à la possibilité pour une Partie de fixer d'autres conditions pour l'utilisation de données par le destinataire (comme des limites à l'usage ou à la diffusion par la Partie destinataire de données à caractère personnel afin d'éviter de nuire à l'enquête menée par la Partie transférante) conformément aux dispositions spécifiques du chapitre II.

265. Lorsqu'elle statue sur une demande de transfert en vertu du paragraphe 10, l'autorité transférante ou désignée est encouragée à tenir dûment compte de tous les facteurs pertinents, comme la gravité de l'infraction pénale, le but dans lequel les données ont été transférées à l'origine, les conditions applicables au transfert originel et le niveau approprié ou non de protection des données à caractère personnel garanti par le pays tiers ou l'organisation internationale concernée.

Paragraphe 11 – Transparence et notification

266. Le paragraphe 11.a impose des conditions de transparence et de notification aux Parties pour les éléments visées aux paragraphes 11.a.i à iv. Ces conditions ont pour but d'aider les personnes concernées à comprendre comment les Parties peuvent être amenées à traiter leurs données. Elles sont aussi destinées à informer les personnes concernées des possibilités d'accès, de rectification et de recours existantes.

267. Chaque Partie dispose d'une latitude pour décider si ces notifications et cette transparence sont assurées par voie de publication de notifications générales à l'attention du public – par exemple sur un site internet gouvernemental – ou par notification personnelle à la personne dont les données à caractère personnel ont été adressées à la Partie destinataire. Ces notifications doivent être facilement accessibles et compréhensibles. Qu'elles soient générales ou personnelles, les notifications doivent comporter les informations suivantes : i) le fondement légal du traitement et ses finalités, y compris les but de la divulgation anticipée ou habituelle, ii) les durées de conservation ou de révision en vertu du paragraphe 5 du présent article, le cas échéant, iii) les destinataires ou catégories de destinataires auxquels les données sont divulguées et iv) les possibilités d'accès, de rectification et de recours judiciaires et non judiciaires existantes.

268. Aux termes du paragraphe 11.b, lorsque la notification est adressée personnellement à la personne dont les données ont été transférées à la Partie destinataire, les conditions de notification et de transparence visées au paragraphe 11.a peuvent faire l'objet de restrictions raisonnables conformément aux conditions énoncées au paragraphe 12.a.i du présent article. Ainsi, en matière pénale, il peut y avoir des circonstances légitimes justifiant de différer ou d'omettre la notification. Ces circonstances sont évoquées au paragraphe 12.a.i et décrites au paragraphe 272 du présent Rapport explicatif. Il peut aussi se produire des situations dans lesquelles le niveau de détail de la notification générale peut être limité, en fonction de la sensibilité des informations.

269. Le paragraphe 11.c offre aux Parties une base d'appréciation pour mettre en balance le souci de transparence et la nécessaire confidentialité dans les affaires pénales. Il dispose que lorsque

le cadre juridique interne de la Partie transférante impose que toute personne dont les données ont été transférées à une autre Partie en vertu du présent Protocole en reçoive personnellement la notification, la Partie transférante prend toutes les mesures nécessaires pour que la Partie destinataire soit informée de cette obligation au moment du transfert et des informations nécessaires. La Partie transférante ne donne pas notification du transfert de données à la personne concernée si la Partie destinataire demande que ce transfert reste confidentiel, lorsque les conditions de restriction fixées au paragraphe 12.a.i s'appliquent. Lorsque de telles conditions aux restrictions ne s'appliquent plus et que notification personnelle peut être donnée à l'intéressé, la Partie destinataire prend des mesures pour que la Partie transférante soit informée que la notification peut être faite. Ces mesures peuvent comprendre un réexamen périodique de l'utilité de ces restrictions. Si elle n'en a pas été informée, la Partie transférante est fondée à adresser des demandes à la Partie destinataire, qui l'informera s'il convient de maintenir la restriction.

Paragraphe 12 – Accès et rectification

270. Le paragraphe 12.a impose à chaque Partie de garantir que toute personne dont elle a reçu les données à caractère personnel en vertu du présent Protocole ait le droit de demander et d'obtenir l'accès à ces données, conformément aux procédures établies dans son cadre juridique interne et sans retard excessif (ce droit pouvant faire l'objet d'éventuelles restrictions), et de les faire rectifier lorsque ces données sont inexactes ou ont fait l'objet d'un traitement indu. L'expression « conformément aux procédures établies dans son cadre juridique interne » donne aux Parties une certaine souplesse quant à la manière dont l'accès aux données et leur rectification peut être demandé et obtenu. L'intention est de renvoyer à des procédures établies, par exemple, par des lois, réglementations, règles (de nature juridictionnelle notamment) et politiques en vigueur ainsi qu'aux règles applicables en matière d'établissement de la preuve. Dans certains systèmes juridiques, la personne concernée devra d'abord chercher à obtenir le droit d'accès et de rectification au niveau administratif avant de passer par la voie judiciaire.

271. Le paragraphe 12.a.i dispose que la personne qui dépose une demande d'accès a le droit d'obtenir une copie écrite ou électronique de la documentation contenant ses données à caractère personnel ainsi que les informations disponibles relatives au fondement juridique et aux finalités du traitement de ces données, de leur conservation et de leurs destinataires ou catégories de destinataires (« l'accès »), ainsi que des informations relatives aux possibilités de recours conformément au paragraphe 13. Cela peut également permettre à l'individu de confirmer si (ou non) ses données personnelles ont été reçues en vertu du Protocole, et ont été ou sont traitées. La communication de la documentation contenant les informations disponibles indiquant le fondement juridique et les finalités du traitement des données aideront la personne concernée à déterminer si les données à caractère personnel sont traitées conformément à la législation applicable. Dans de nombreuses Parties, le cadre prévoyant l'accès à ces informations peut déjà être fourni par leur législation relative à la vie privée, à la liberté d'information ou à l'accès aux dossiers administratifs.

272. L'obtention de cet accès peut, dans des cas particuliers, être soumise à des restrictions proportionnées autorisées par le cadre juridique interne d'une Partie, ces restrictions devant être « nécessaires, au moment de la décision, pour protéger les droits et libertés d'autrui ou d'importants objectifs d'intérêt public général et [tenir] dûment compte des intérêts légitimes de la personne concernée ». Les droits et libertés d'autrui peuvent, par exemple, comprendre la vie privée d'autres personnes dont les données à caractère personnel seraient révélées si l'accès était accordé. Les objectifs d'intérêt public général importants peuvent, par exemple, être la protection de la sûreté nationale et de la sécurité publique (ce qui concerne, par exemple, les informations relatives à des menaces terroristes potentielles ou à des risques sérieux pour les membres des forces de l'ordre), la prévention, la détection, l'instruction ou la poursuite d'infractions pénales et la nécessité d'éviter de nuire aux enquêtes, informations judiciaires et procédures officielles. Dans ce contexte, les « restrictions proportionnées » doivent être appliquées par chaque Partie conformément aux principes correspondants de son ordre juridique interne, dans un sens similaire à celui donné dans l'explication du principe de proportionnalité au paragraphe 146 du Rapport explicatif de la

Convention. Pour les Parties à la Convention européenne des droits de l'homme et au Protocole d'amendement (STCE n° 223) à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108), la proportionnalité découlera des obligations imposées par ces conventions. Les autres parties appliqueront les principes correspondants de leur ordre juridique interne qui limitent raisonnablement la possibilité d'obtenir l'accès pour protéger d'autres intérêts légitimes. Comme indiqué ci-dessus, les restrictions proportionnées doivent protéger les droits et libertés d'autrui ou protéger des objectifs importants d'intérêt public général et tenir dûment compte des "intérêts légitimes de la personne concernée". L'expression "intérêts légitimes de la personne concernée" a été considérée par les rédacteurs comme incluant les droits et libertés de la personne. Dans les cas où ces motifs de restriction sont invoqués, l'autorité requise est encouragée à étayer cette décision aux fins du paragraphe 14. Les Parties devraient également considérer la possibilité d'accorder un accès partiel lorsque les motifs de restriction (par exemple dans le but de protéger des informations commerciales confidentielles ou classifiées) ne s'appliquent qu'à certaines parties des informations concernées.

273. Lorsque d'autres dispositions de cet article permettent des restrictions dans les conditions exposées au paragraphe 12.a.i, l'expression « au moment de la décision » renvoie, dans le cas du paragraphe 7, au moment de la notification de l'incident de sécurité et, dans le cas du paragraphe 11.b, au moment où une Partie demande la confidentialité.

274. En vertu du paragraphe 12.a.ii., une personne est fondée à demander et à obtenir la rectification de ses données à caractère personnel, conformément aux procédures établies en droit interne et sans délai indu, lorsque ces données sont inexactes ou ont été indûment traitées. Cette rectification consistera notamment – selon ce qui convient et ce qui est raisonnable au vu des motifs justifiant la rectification et le contexte particulier du traitement – à corriger les données, à les compléter (par exemple par des annotations, des informations complémentaires ou des corrections), à les effacer ou à les anonymiser, à en restreindre le traitement ou à les bloquer. À cet égard, les rédacteurs ont considéré que l'effacement ou l'anonymisation est la solution appropriée et raisonnable dans le cas où les données sont traitées en violation du paragraphe 5. En cas de violation du paragraphe 2, il peut aussi être approprié que la Partie restreigne le traitement ; cependant, cela dépendra en fin de compte du contexte particulier (par exemple de la nécessité de conserver les données à caractère personnel aux fins de l'établissement de la preuve). Lorsque les données sont anonymisées, les Parties devraient prendre en considération le risque d'une réidentification non autorisée et envisager d'appliquer des mesures appropriées pour limiter autant que possible ce risque. Les Parties sont encouragées à notifier, lorsque c'est possible, à la Partie transférante et aux autres entités auxquelles les données ont été communiquées toutes les mesures de rectification prises.

275. Aux termes du paragraphe 12.b, en cas de refus ou de limitation de l'accès ou de la rectification visés au paragraphe 12.a, la Partie informe la personne concernée de ce refus ou de cette limitation par écrit, y compris par voie électronique, et sans retard indu. Si l'autorité doit motiver ce refus ou cette limitation, la communication peut être générale (c'est-à-dire qu'elle peut ne pas confirmer ou dénier l'existence d'un dossier correspondant) dans les cas où cela est nécessaire pour ne pas compromettre un objectif, conformément au paragraphe 12.a.i. Les Parties doivent cependant veiller à ce que cette communication donne des informations sur les possibilités de recours existantes.

276. Les Parties peuvent facturer des frais d'accès (par exemple pour les coûts administratifs liés à la compilation et à l'examen de documents auxquels l'accès a été demandé). Toutefois, les frais éventuels doivent rester dans les limites du raisonnable et ne pas être excessifs au vu des ressources impliquées afin de ne pas dissuader ou décourager les intéressés de faire une demande d'accès. Pour faciliter l'exercice des droits énoncés au paragraphe 12.a, les Parties sont encouragées à autoriser les personnes concernées à se faire assister par un représentant pour demander et obtenir les mesures qui y sont décrites ou pour déposer une demande et/ou une réclamation en leur nom. Dans ces circonstances, les notifications faites en application du paragraphe 11.a ainsi que les

informations obtenues en réponse à une demande d'accès en vertu du paragraphe 12.a.i. pourront mentionner cette possibilité. Cette représentation doit cependant être conforme aux conditions prescrites par le droit interne applicable de la Partie à laquelle ces mesures sont demandées, ou la requête et/ou la plainte est déposée comme décrit ci-dessus, notamment pour ce qui est des conditions dans lesquelles des personnes ou entités peuvent représenter les intérêts légaux de tiers (comme les règles régissant la procuration dans certains systèmes juridiques nationaux).

Paragraphe 13 – Recours judiciaire et non judiciaire

277. Le paragraphe 13 dispose que « [c]haque partie dispose d'un système permettant d'offrir des recours judiciaires et non judiciaires effectifs pour assurer la réparation des violations des garanties énoncées dans le présent article ». Il appartient à chaque Partie de déterminer les types de recours ouverts pour les violations des dispositions de cet article. Il n'est pas obligatoire que chaque type de recours soit ouvert pour chaque violation de cet article. Les voies de recours prévues pour remédier aux violations du présent article doivent être effectives. Les Parties peuvent prévoir, lorsque la situation s'y prête, le dédommagement comme moyen de réparation de préjudices matériels ou non matériels pour lesquels le plaignant a établi qu'ils résultent de la violation concernée.

Paragraphe 14 – Supervision

278. Le paragraphe 14 exige des Parties qu'elles « dispose[nt] d'une ou de plusieurs autorités publiques qui, ensemble ou séparément, exercent des fonctions et des compétences de supervision indépendantes et effectives à l'égard des mesures établies dans le présent article ». Cette disposition laisse aux Parties toute latitude sur la manière de mettre en œuvre cette obligation. Certaines pourront établir des autorités spécialisées dans la protection des données tandis que d'autres pourront choisir de faire exercer cette supervision concurremment par plusieurs autorités, dont les fonctions peuvent se recouper, reflétant ainsi les différences de structures constitutionnelles, organisationnelles et administratives entre les Parties. Dans certaines d'entre elles, ces autorités de supervision pourront être établies au sein des structures gouvernementales dont elles supervisent les activités, leur budget faisant partie du budget global de ces structures. Dans ce cas, ces autorités devraient jouir de l'indépendance nécessaire pour pouvoir s'acquitter effectivement de leurs responsabilités de supervision.

279. Les rédacteurs ont considéré que plusieurs éléments contribuent à l'indépendance et à l'effectivité des fonctions et compétences de supervision. Ainsi, ces autorités devraient remplir leur mission et exercer leurs compétences de manière impartiale. Elles devraient pouvoir agir en étant dégagées de toute influence extérieure susceptible d'interférer dans l'exercice indépendant de leurs fonctions et compétences. Elles ne devraient, en particulier, recevoir aucune instruction, dans une affaire donnée, portant sur l'exercice de leurs compétences en matière d'enquête et/ou sur la prise de mesures correctives. Enfin, il est important qu'elles disposent des compétences, des connaissances et de l'expertise nécessaires pour mener à bien leurs tâches et qu'elles soient dotées des ressources financières, techniques et humaines appropriées pour pouvoir exercer effectivement leurs fonctions.

280. Les fonctions et compétences de ces autorités « comprennent des pouvoirs d'enquête, le pouvoir de donner suite aux plaintes, et la capacité de prendre des mesures correctives ». Les rédacteurs ont considéré que les pouvoirs d'enquête devraient inclure le pouvoir d'obtenir les informations nécessaires pour que ces autorités puissent mener à bien leurs tâches, notamment l'accès, sous réserve des conditions appropriées, aux registres tenus en vertu du paragraphe 8. Les actions correctives pourront inclure des avertissements en cas de non-conformité ou des consignes pour assurer la conformité des opérations de traitement des données (exigeant par exemple la mise en œuvre de mesures supplémentaires de sécurité pour limiter l'accès aux données ou la rectification de données à caractère personnel), l'imposition de la suspension (temporaire) de certaines opérations de traitement, ou le renvoi de la question à d'autres autorités (par exemple à des services

d'inspection générale, des procureurs, des juges d'instruction ou des instances législatives). Ces mesures correctives peuvent être prises de la propre initiative des autorités ou à la suite de plaintes déposées par des personnes concernant le traitement de leurs données à caractère personnel.

281. Les Parties sont encouragées à promouvoir la coopération entre leurs autorités de surveillance respectives. Des consultations entre les autorités respectives des Parties dans l'exercice de leurs fonctions de surveillance en vertu du présent article peuvent avoir lieu, le cas échéant. Cela peut inclure l'échange d'informations et de meilleures pratiques.

Paragraphe 15 – Consultation et suspension

282. Le paragraphe 15 régit les situations dans lesquelles une Partie est fondée, aux termes de l'article 14 à suspendre le transfert de données à caractère personnel à une autre Partie en vertu du présent Protocole lorsque les Parties agissent en application du paragraphe 1.a du présent article. Étant donné l'importance des finalités répressives du présent Protocole, le paragraphe 15 établit clairement que cette suspension ne devrait intervenir que dans le cadre de conditions strictes et conformément aux procédures spécifiques qu'il décrit. Le but des dispositions du présent article relatives à la protection des données est d'offrir les garanties appropriées pour la protection des données à caractère personnel, y compris lorsqu'elles font ensuite l'objet d'un partage avec d'autres instances au sein d'une même Partie et d'autres transferts. Les rédacteurs ont considéré que les garanties apportées par le présent article et leur mise en œuvre effective sont essentielles et qu'il est donc important de prévoir la suspension des transferts de données à caractère personnel dans certaines situations. En conséquence, une Partie peut suspendre le transfert vers une autre Partie de données à caractère personnel effectué en vertu du présent Protocole s'il a des preuves substantielles d'une violation systématique ou flagrante des termes du présent article ou de l'imminence d'une violation flagrante. Si la condition de la « preuve substantielle » n'impose pas à une Partie de démontrer l'existence indubitable d'une violation systématique ou flagrante, cette Partie ne peut pas suspendre les transferts en se fondant sur de simples soupçons ou conjectures. Sa décision doit bien plutôt être solidement fondée sur des éléments de preuve factuels crédibles. Une « violation flagrante » est une violation conséquente d'une obligation importante au titre du présent article. Il peut s'agir de l'absence, dans le cadre juridique interne d'une Partie, d'une garantie requise en vertu du présent article. Les rédacteurs ont reconnu que la suspension est aussi possible en raison de violations systématiques, par exemple de violations fréquentes des garanties apportées par cet article. Ils ont en outre reconnu que la non-application de certaines garanties lors du traitement de données à caractère personnel dans un cas donné ne constitue pas une raison suffisante, en l'absence d'une violation flagrante, pour invoquer cette disposition car la personne concernée devrait pouvoir demander réparation de ces violations par des voies de recours judiciaires et non judiciaires effectives en vertu du paragraphe 13 de l'article 14.

283. Le Paragraphe 15 dispose en outre que « [c]ette suspension n'interviendra qu'à l'expiration d'un préavis raisonnable et après que les Parties auront mené des consultations d'une durée raisonnable sans parvenir à une solution ». Cette obligation de consultations dispose que la suspension de transferts essentiels à des fins de répression ne devrait intervenir qu'après avoir donné à l'autre Partie une possibilité raisonnable de clarifier la situation ou de remédier aux inquiétudes exprimées. À l'ouverture de ces consultations, la Partie qui invoque le présent paragraphe peut demander à l'autre Partie de lui fournir les informations pertinentes. Toutefois, comme le reconnaît le paragraphe 15, la Partie qui invoque ce paragraphe doit disposer de preuves substantielles d'une violation flagrante ou systématique ou de l'imminence d'une violation flagrante. Le mécanisme de consultations ne doit donc pas être utilisé pour collecter d'autres preuves lorsqu'il n'y a que des soupçons de violation. Les transferts de données effectués en vertu du présent Protocole ne peuvent être suspendus qu'après un préavis raisonnable et l'échec de consultations d'une durée raisonnable. Toutefois, une Partie peut suspendre provisoirement les transferts en cas de violation systématique ou flagrante présentant un risque important et imminent pour la vie ou la sécurité d'une personne physique ou de préjudice financier ou de réputation pour cette personne. Est également visée l'existence d'un risque important et imminent de préjudice pour l'intégrité

corporelle ou la santé d'une personne physique. Dans ces cas, la Partie adresse une notification à l'autre Partie et entame des consultations avec elle dès l'application de la suspension provisoire des transferts. Les rédacteurs ont considéré que la suspension provisoire devrait, de manière générale, être limitée aux transferts directement concernés par les motifs justifiant la suspension provisoire.

284. Si la Partie qui procède à la suspension remplit les conditions fixées au paragraphe 15, elle peut suspendre les transferts sans que l'autre Partie puisse faire de même. Toutefois, si cette autre Partie a la preuve substantielle que la suspension n'était pas conforme aux termes de l'article 15, elle peut à son tour suspendre les transferts vers la Partie qui a décidé la suspension. Dans ce contexte, l'expression « preuve substantielle » a le même sens que dans le cas de la suspension initiale. La suspension décidée par la première Partie serait incompatible avec le paragraphe 15 dans le cas où cette Partie n'a pas de « preuve substantielle », que la violation n'est ni « systématique » ni « flagrante » ou que cette Partie n'a pas satisfait aux conditions procédurales de la suspension, en particulier pour ce qui est des consultations.

285. Enfin, le paragraphe 15 dispose que « la Partie qui a procédé à la suspension lève cette dernière dès qu'il a été remédié à la violation justifiant la suspension » et que « toute suspension réciproque est levée à ce moment ». Une règle similaire à celle prévue à l'article 24, paragraphe 4, s'applique en cas de suspension en vertu du présent paragraphe, à savoir que « toute les données à caractère personnel transférées avant la suspension continuent à être traitées conformément au présent Protocole ».

286. Les Parties sont encouragées à notifier officiellement aux fournisseurs de services et aux entités auxquels des demandes ou des injonctions peuvent être adressées en vertu de la section 2 du chapitre II toute suspension ou suspension provisoire en vertu du présent paragraphe ou à rendre publiques ces demandes ou ces injonctions. Cette communication peut être importante pour suspendre effectivement les transferts de données à caractère personnel à une Partie qui viole systématiquement ou de manière flagrante le présent article, mais aussi pour assurer que les fournisseurs de services et les entités ne limitent pas le transfert d'informations ou de preuves en vertu du présent Protocole parce qu'ils pensent à tort qu'une Partie fait l'objet d'une suspension provisoire.

287. Bien que le paragraphe 15 prévoie des procédures spécifiques relatives aux consultations et à la suspension des transferts de données à caractère personnel pour des raisons de protection des données, ces procédures n'ont pas pour but de modifier les dispositions de l'article 23, paragraphe 1, relatives aux consultations, ni les droits de suspension qui peuvent être applicables à d'autres articles du présent Protocole en vertu du droit international.

Chapter IV – Clauses finales

288. Les dispositions du présent chapitre s'inspirent essentiellement à la fois du « Modèle de clauses finales pour les conventions, protocoles additionnels et protocoles d'amendement conclus au sein du Conseil de l'Europe », qui a été adopté par le Comité des Ministres lors de la 1291e réunion des Délégués des Ministres tenue en juillet 2017, et des clauses finales de la Convention. Étant donné que certains des articles du présent chapitre reprennent le libellé du modèle de clauses finales ou s'inspirent de la longue pratique conventionnelle du Conseil de l'Europe, ils n'appellent pas de commentaires particuliers. Toutefois, certaines modifications du modèle de clauses finales et des clauses finales de la Convention sur la cybercriminalité méritent une explication.

Article 15 – Effets de ce Protocole

289. Le paragraphe 1.a de l'article 15 incorpore l'article 39, paragraphe 2, de la Convention. Ce paragraphe dispose que les Parties sont libres d'appliquer des accords préexistants ou qui pourraient entrer en vigueur à l'avenir, comme le reconnaît le paragraphe 312 du Rapport explicatif de la Convention. Le Protocole, tout comme la Convention, pose généralement des obligations minimales. Ce paragraphe reconnaît par conséquent que les Parties sont libres de souscrire des obligations plus spécifiques, en plus de celles déjà fixées dans le Protocole, lorsqu'elles établissent leurs relations au sujet des questions traitées dans ce dernier. Toutefois, les Parties sont tenues, ce faisant, de respecter les objectifs et principes du Protocole et ne peuvent donc accepter d'obligations qui iraient à l'encontre du but de ce dernier.

290. Le paragraphe 1.b de cet article reconnaît aussi l'intégration accrue de l'Union européenne (UE) depuis l'ouverture de la Convention à la signature, en 2001, en particulier dans les domaines de la coopération policière et judiciaire et de la protection des données. Il autorise, par conséquent, les États membres à appliquer entre eux le droit de l'Union européenne qui régit les questions traitées par le Protocole. Pour les rédacteurs, le droit de l'Union européenne s'entend des mesures, principes et procédures prévues par l'ordre juridique de l'UE, en particulier ses lois, règlements et dispositions administratives, ainsi que les autres mesures contraignantes, dont les décisions de justice. Le but du paragraphe 1.b est donc de couvrir les relations internes entre les États membres de l'Union européenne et entre ses États membres, ses institutions, ses organes et ses agences. En l'absence de dispositions législatives de l'Union européenne sur une question entrant dans le champ d'application du présent Protocole, celui-ci continuerait de régir la question concernée entre les Parties qui sont membres de l'UE.

291. Le paragraphe 1.c précise que le paragraphe 1.b ne porte nullement atteinte à la pleine application du présent Protocole entre les Parties qui sont membres de l'UE et d'autres Parties. Le paragraphe 1.b n'a donc pas pour but de produire un quelconque effet au-delà des relations internes à l'UE telles que décrites au paragraphe 290 ci-dessus. Le Protocole s'applique pleinement entre les Parties qui sont membres de l'UE et les autres Parties. Les rédacteurs ont jugé cette disposition essentielle pour garantir que les Parties qui ne sont pas membres de l'UE bénéficieraient pleinement du Protocole dans leurs relations avec des Parties membres de l'UE. Ainsi, les rédacteurs ont débattu du fait de savoir si un État membre de l'UE qui reçoit des informations ou des preuves d'une Partie qui n'est pas membre de l'UE devrait chercher à obtenir le consentement de cette dernière avant de transférer les informations ou preuves en question à une autre Partie membre de l'UE, conformément à l'article 14, paragraphe 10. De même, le paragraphe 1.a de cet article s'appliquerait pleinement entre les Parties qui sont membres de l'UE et les Parties qui ne le sont pas.

292. Le paragraphe 2 de cet article incorpore l'article 39, paragraphe 3, de la Convention. Pas plus que la Convention, comme exposé au paragraphe 314 de son Rapport explicatif, le présent Protocole n'a pour but de traiter toutes les questions concernant les diverses formes de coopération entre les Parties ou entre les Parties et des entités privées en matière de cybercriminalité et de collecte de preuves d'infractions pénales sous forme électronique. Par conséquent, le paragraphe 2 de cet

article a été inséré pour qu'il soit clair que le Protocole n'a d'effet que sur les questions dont il traite. Il ne saurait avoir d'incidence sur les autres droits, restrictions, obligations et responsabilités qui peuvent exister mais qu'il ne règle pas.

293. Cet article ne comporte pas de disposition analogue à l'article 39, paragraphe 1, de la Convention. Cette disposition de la Convention explique que l'objet de la Convention était de compléter des traités ou accords bilatéraux applicables entre les Parties, notamment certains traités d'extradition et d'entraide. Le présent Protocole ne comprend aucune disposition d'extradition et nombre de ses dispositions ne concernent pas l'entraide. Comme exposé plus en détail à l'article 5 et dans le rapport explicatif correspondant, les modes d'interaction entre chacune des sections du chapitre II relatives aux mesures de coopération et les traités d'entraide sont variables. Par conséquent, les rédacteurs ont estimé qu'il était inutile d'inclure une disposition similaire à celle de l'article 39, paragraphe 1.

Article 16 – Signature et entrée en vigueur

294. Le présent article autorise toutes les Parties à la Convention à signer le présent Protocole et à devenir Parties à ce dernier. À la différence du Premier Protocole (article 11), le présent Protocole ne prévoit pas de procédure d'adhésion au présent Protocole. Un État souhaitant signer le présent Protocole et devenir Partie à ce dernier devra d'abord devenir Partie à la Convention.

295. Le paragraphe 3 dispose que le présent « Protocole entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Parties à la Convention auront exprimé leur consentement à être liées par le présent Protocole. » Alors que l'article 36 de la Convention prévoyait qu'au moins trois des cinq Parties devaient être des États membres du Conseil de l'Europe pour que la Convention entre en vigueur, cette condition n'est pas prévue ici car il s'agit d'un Protocole additionnel à une Convention et toutes les Parties doivent avoir le même droit d'appliquer le présent Protocole dès qu'un nombre minimal de cinq Parties à la Convention auront exprimé leur consentement à être liés par lui. C'est l'approche suivie par l'article 10 du Premier Protocole.

296. Le paragraphe 4 décrit le processus d'entrée en vigueur du présent Protocole pour les Parties à la Convention qui exprimeront leur consentement à être liées par ce dernier après son entrée en vigueur conformément au paragraphe 3. C'est l'approche suivie par l'article 36, paragraphe 4, de la Convention.

Article 17 – Clause fédérale

297. L'article 17 du présent Protocole comporte une clause fédérale similaire à celle de l'article 41 de la Convention, qui permet à un État fédéral partie au Protocole de formuler une réserve pour assurer la cohérence avec « [les] principes fondamentaux régissant les relations entre son gouvernement central et les États constituants ou autres entités territoriales similaires ». Le but de l'article 17 est le même que celui de l'article 41 de la Convention, qui est, comme exposé au paragraphe 316 du rapport explicatif de la Convention, « de trouver un arrangement concernant les difficultés que des États fédéraux risquent de rencontrer en raison de la répartition typique des pouvoirs entre les autorités fédérales et régionales ».

298. Les États fédéraux sont autorisés à faire des réserves concernant les obligations découlant du chapitre II de la Convention (établissement des infractions pénales et des mesures procédurales en droit interne) lorsque ces mesures ne relèvent pas des compétences du gouvernement central de l'État fédéral. Toutefois, il est attendu des États fédéraux qu'ils soient en mesure d'offrir une coopération internationale aux autres Parties en vertu du chapitre III de la Convention.

299. Bien que le présent Protocole porte sur la coopération internationale plutôt que sur des mesures de droit interne, les négociateurs ont reconnu qu'il reste nécessaire d'y faire figurer une

clause fédérale. Si la Convention ne prévoyait pas la possibilité de faire des réserves liées au fédéralisme en matière d'entraide judiciaire, la majorité des mesures prévues par le présent Protocole ne fonctionnent pas de la même manière que dans le cadre de l'entraide classique. Le Protocole prévoit plusieurs mesures de coopération d'une efficacité supérieure à l'entraide classique et qui ne nécessitent pas forcément de passer par le gouvernement central. Il introduit en particulier deux mesures, aux articles 6 et 7, permettant aux autorités compétentes d'une Partie de chercher à coopérer directement avec des entreprises privées établies dans une autre Partie. Ces dispositions nécessitent le respect de certaines mesures procédurales qu'un État fédéral pourrait avoir du mal à imposer aux autorités compétentes d'États constituants ou d'autres entités territoriales similaires. Ainsi, l'article 7 prévoit qu'une Partie peut, moyennant notification au Secrétaire Général, exiger des autorités d'autres Parties qu'elles avisent immédiatement une autorité gouvernementale désignée à cet effet de toute injonction adressée à un fournisseur de services pour obtenir des informations relatives aux abonnés. D'autres articles imposent de prendre des mesures législatives ou autres qu'un État fédéral peut ne pas être en situation de pouvoir exiger de ses États constituants ou entités territoriales similaires. Enfin, le présent Protocole comprend des dispositions détaillées relatives à la protection des données, ce qui n'est pas le cas de la Convention. Aux États-Unis par exemple, en vertu de la Constitution et des principes fondamentaux du fédéralisme, les États constituants adoptent leurs propres lois pénales et lois de procédure pénale (distinctes des lois fédérales) ; ils établissent leurs propres tribunaux, procureurs et services de police et conduisent les enquêtes et poursuites concernant les infractions à leur législation pénale. Les autorités compétentes des États sont indépendantes des autorités fédérales, auxquelles elles ne sont pas subordonnées.

300. Lorsque les autorités d'un État constituant ou d'une entité territoriale similaire d'un État fédéral souhaitent bénéficier des formes de coopération prévues par le présent Protocole, il se peut 1°) que leurs lois procédurales et relatives à la protection de la vie privée diffèrent de celles appliquées par les autorités du gouvernement central, 2°) qu'elles ne soient pas soumises hiérarchiquement au gouvernement central, ou 3°) que le gouvernement central n'ait pas légalement compétence pour diriger leurs actions. Dans ces situations, la seule assurance qu'il pourrait y avoir qu'un État constituant ou une entité territoriale similaire se conforme aux prescriptions du présent Protocole – en ce qui concerne la collecte d'informations ou de preuves ainsi que leur traitement subséquent – serait (a) qu'il les appliquent lui-même ou (b) que ses autorités cherchent à obtenir la coopération par l'intermédiaire des autorités du gouvernement central, ou avec leur participation, lesquelles veilleraient alors au respect de ces obligations (par exemple par le biais de l'entraide ou du point de contact 24/7, ou par la participation du gouvernement central à une équipe commune d'enquête).

301. Au vu de ces considérations, le paragraphe 1 prévoit une possibilité pour les États fédéraux parties au Protocole de faire des réserves. Ils peuvent se réserver le droit d'assumer les obligations découlant du présent Protocole conformément à leurs principes fondamentaux régissant les relations entre leur gouvernement central et leurs États constituants ou autres entités territoriales similaires, sous réserve des paragraphes 1.a à c, qui limitent la portée de ces réserves. En vertu du paragraphe 1.a, le gouvernement central d'un État fédéral qui fait une telle réserve est tenu d'appliquer toutes les dispositions du présent Protocole (sans préjudice des réserves et déclarations possibles). Dans le cas des Parties pour lesquelles les obligations relatives à la protection des données prévues par le présent Protocole sont régies par l'article 14, paragraphe 1.a, cela comprend les obligations énoncées à l'article 14, paragraphe 9.b, relatives au partage des données avec des États constituants ou d'autres entités territoriales similaires (voir le paragraphe 237 du rapport explicatif) lorsqu'une autorité fédérale a demandé des informations en vertu du présent Protocole soit pour ses propres fins, soit pour le compte d'une autorité de niveau inférieur à l'échelon fédéral et partage ensuite ces informations avec cette autorité. De plus, le paragraphe 1.b prévoit, tout comme l'article 41, paragraphe 1, de la Convention que ces réserves sont sans effet sur l'obligation d'un État fédéral partie à la Convention de répondre aux demandes de coopération d'autres Parties conformément aux dispositions du chapitre II. Enfin, en vertu du paragraphe 1.c et sans préjudice des réserves faites par un État fédéral, l'article 13 du présent Protocole - qui exige, conformément à l'article 15 de la Convention, que le droit interne garantisse la protection des droits de l'homme et

des libertés - s'applique, outre à l'État fédéral lui-même en vertu du paragraphe 1.a, également aux États constituants ou entités territoriales similaires.

302. Le paragraphe 2 dispose que dans les cas où un État fédéral fait des réserves en vertu du paragraphe 1 et que les autorités d'un État constituant ou d'une entité territoriale similaire de cette Partie demande la coopération directe d'une autorité, d'un fournisseur de services ou d'une entité située dans une autre Partie, cette dernière « peut empêcher les autorités, les fournisseurs ou les entités sur son territoire de coopérer en réponse à [cette] demande ». Cette autre Partie peut déterminer de quelle manière empêcher les autorités, fournisseurs de services ou entités sur son territoire de coopérer. Il y a deux exceptions à la possibilité d'une Partie d'empêcher la coopération :

303. Premièrement, le paragraphe 2 dispose que la coopération ne peut pas être empêchée par cette autre Partie si l'État fédéral concerné a, du fait que l'État constituant ou autre entité territoriale similaire remplit les obligations du présent Protocole, « notifié au Secrétaire Général du Conseil de l'Europe que l'État constitutif ou autre entité territoriale similaire s'est engagé à appliquer les obligations du présent Protocole applicables à cet État fédéral ». L'expression « obligations du présent Protocole applicables à cet État fédéral » signifie qu'une autorité d'un État constituant ou autre entité territoriale similaire ne peut être soumise à une obligation auquel le gouvernement central ne serait pas soumis, notamment une réserve applicable. Si l'État fédéral a adressé cette notification au Secrétaire Général pour un État constituant particulier, une autre Partie devra répondre à une injonction ou à une demande de cet État de la même manière que si elle lui avait été adressée par des autorités du gouvernement central. Les obligations et procédures prévues pour chaque mesure de coopération du chapitre II continuent naturellement de s'appliquer aux demandes et injonctions soumises par ces États constituants ou entités territoriales similaires. Le respect de ces obligations est nécessaire. Le présent paragraphe prévoit que le Secrétaire Général du Conseil de l'Europe établit et tient un registre de ces notifications. Les Parties sont encouragées à communiquer des informations actualisées au Secrétaire Général.

304. Deuxièmement, en vertu du paragraphe 3, si une demande ou une injonction d'un État constituant ou d'une autre entité territoriale similaire a été transmise par l'intermédiaire du gouvernement central ou conformément à un accord d'établissement d'une équipe d'enquête commune en vertu du paragraphe 3 auquel participe le gouvernement central, une Partie destinataire d'une demande de coopération ne peut pas empêcher les autorités, fournisseurs de services ou entités de son territoire de transférer des informations ou des preuves conformément aux dispositions du présent Protocole au motif que la coopération est demandée par un État constituant ou une entité territoriale similaire d'un État fédéral qui a fait des réserves au titre du paragraphe 1. En effet, lorsque la demande ou l'injonction est soumise par l'intermédiaire du gouvernement central ou que l'accord établissant l'équipe commune d'enquête a été conclu avec sa participation, c'est à lui qu'il incombe alors « [d']assure[r] l'exécution des obligations applicables du Protocole ». Puisque le gouvernement central transmet la demande ou l'injonction (ou participe à l'ECE), il a la possibilité et l'obligation de vérifier le respect des conditions posées par le Protocole en ce qui concerne ces mesures. Ainsi, lorsque notification doit être donnée à une autre Partie, en vertu de l'article 7, paragraphe 5.a, de la transmission d'une injonction pour l'obtention d'informations relatives aux abonnés, c'est au gouvernement central qu'il incombe d'adresser cette notification. En matière de protection des données (pour les Parties auxquelles l'article 14, paragraphe 1.a est applicable), lorsqu'un État constituant ou une autre entité territoriale similaire fait une demande de coopération par l'intermédiaire du gouvernement central, celui-ci lui communique les données et est tenu de se conformer aux exigences de l'article 1, paragraphe 9.b (partage des données à l'intérieur d'une Partie). Le gouvernement central doit donc mettre en place des mesures pour que les autorités destinataires des données continuent de les protéger efficacement en assurant un niveau de protection comparable à celui voulu par l'article 14. Les autorités d'un État constituant ou d'une entité territoriale similaire qui demandent et reçoivent des données personnelles de cette manière ne sont sinon pas tenues d'appliquer l'article 14. Si les Parties concernées appliquent un autre accord ou arrangement visé à l'article 14, paragraphes 1.b ou 1.c, les termes applicables de ces accords ou arrangements s'appliquent.

305. Le paragraphe 4 reprend la formulation de l'article 41, paragraphe 3 de la Convention et a les mêmes effets. Ainsi, s'agissant des dispositions de la Convention dont l'application relève de la compétence des États constituants ou autres entités territoriales similaires (sauf notification adressée au Secrétaire Général du Conseil de l'Europe conformément au paragraphe 2 du présent article), le gouvernement central de l'État fédéral est tenu : 1°) d'informer les autorités de ses États constituants ou autres entités territoriales similaires des dispositions du présent Protocole, et 2°) de donner « son avis favorable, en les encourageant à prendre les mesures appropriées pour leur donner effet », incitant ainsi les États constituants ou entités territoriales similaires à appliquer pleinement le présent Protocole. Aux fins du Protocole, le but est aussi de permettre finalement que ces États constituants ou autres entités territoriales similaires reçoivent les notifications prévues au paragraphe 2 de cet article.

Article 18 – Application territoriale

306. L'article 38 de la Convention permet aux Parties de préciser le ou les territoires auxquels la Convention s'appliquerait. Cet article applique automatiquement le Protocole aux territoires spécifiés par une Partie en vertu de l'article 38, paragraphe 1 ou 2, de la Convention dans la mesure où cette déclaration n'a pas été retirée en vertu de l'article 38, paragraphe 3, de la Convention. Les rédacteurs ont estimé qu'il serait préférable que la Convention et le Protocole aient le même champ d'application territorial comme règle par défaut.

307. Le paragraphe 2 de cet article dispose qu' « [une] Partie peut, au moment de la signature de ce Protocole ou au moment du dépôt de son instrument de ratification, d'acceptation ou d'approbation, préciser que le présent Protocole ne s'applique pas à un ou plusieurs territoires spécifiés dans les déclarations de la Partie en vertu des paragraphes 1 ou 2 de l'article 38 de la Convention ». Conformément au paragraphe 3, les Parties peuvent retirer la déclaration faite en vertu du paragraphe 2 de cet article, selon les modalités précisées; le retrait de la déclaration faite au paragraphe 2 aurait pour effet d'appliquer le Protocole à des territoires supplémentaires qui étaient couverts par la Convention mais auxquels le Protocole n'avait pas été appliqué auparavant.

308. Cet article ne permet pas d'appliquer le Protocole aux territoires non couverts par la Convention.

Article 19 – Réserves et déclarations

309. Le présent article prévoit un certain nombre de cas où il est possible de formuler des réserves. Étant donné la portée mondiale de la Convention et le fait qu'il s'agit d'obtenir le même nombre d'adhésions pour le présent Protocole, ces réserves permettent aux Parties à la Convention de devenir Parties au présent Protocole, tout en leur permettant de conserver certaines approches et notions compatibles avec leur législation interne ou à leurs principes juridiques fondamentaux, selon le cas.

310. Les possibilités de faire des réserves sont limitées afin de garantir autant que faire se peut l'application uniforme du présent Protocole par les Parties. C'est pourquoi celles-ci ne peuvent faire aucune autre réserve que celles qui sont énumérées. De plus, une Partie à la Convention ne peut faire une réserve qu'au moment de la signature de ce Protocole ou du dépôt de son instrument de ratification, d'acceptation ou d'approbation.

311. Comme pour la Convention, les réserves au présent Protocole visent à exclure ou à modifier l'effet juridique d'obligations énoncées dans le présent Protocole (voir le paragraphe 315 du rapport explicatif de la Convention). Dans le présent Protocole, les Parties sont autorisées à exclure toute une forme de coopération. En particulier, l'Article 7, paragraphe 9.a, permet à une Partie de se réserver le droit de ne pas appliquer cet article dans son intégralité. Il est également possible de formuler des réserves pour exclure la coopération concernant tout un article portant sur un certain type de données. C'est ainsi que l'article 7, paragraphe 9.b, autorise une Partie à se réserver le

droit de ne pas appliquer l'article 7 à certains types de numéros d'accès si la divulgation de ces numéros devait être incompatible avec les principes fondamentaux de sa loi nationale. De même, l'article 8, paragraphe 13, autorise une Partie à se réserver le droit de ne pas appliquer cet article aux données relatives au trafic.

312. Le présent article porte également sur les déclarations. Comme dans le cas de la Convention, les Parties sont autorisées, par le moyen des déclarations faites dans le cadre du présent Protocole, à insérer certaines procédures supplémentaires spécifiées qui modifient la portée des dispositions. Ces procédures supplémentaires ont pour objet de tenir compte de certaines différences théoriques, juridiques ou pratiques, ce qui se justifie au vu de la portée mondiale de la Convention et de l'aspiration à donner au présent Protocole une portée équivalente. Les déclarations énumérées appartiennent généralement à deux catégories:

313. Les déclarations appartenant à la première catégorie autorisent une Partie à déclarer que certains pouvoirs ou mesures doivent être exercés ou appliqués par certaines autorités ou que la coopération doit être assurée par certaines voies. C'est le cas de l'article 10, paragraphe 9 (permettant de déclarer que les demandes peuvent être adressées à des autorités autres que l'autorité centrale); de l'article 12, paragraphe 3 (l'accord relatif à l'équipe commune d'enquête doit être conclu par l'autorité centrale); de l'article 8, paragraphe 11 (une Partie faisant une déclaration peut exiger que les demandes des autres Parties soumises en vertu de cet article soient transmises par les autorités centrales).

314. Les déclarations appartenant à la deuxième catégorie autorisent les Parties à exiger la prise de mesures procédurales distinctes ou supplémentaires concernant certaines mesures ou formes de coopération afin de respecter le droit interne ou d'empêcher que les autorités ne soient submergées. Ainsi, par exemple, l'article 7, paragraphe 8, et l'article 9, paragraphe 1.b, autorisent une Partie à faire des déclarations tendant à exiger la prise de certaines mesures procédurales concernant les données relatives aux abonnés. L'article 7, paragraphes 2.b et 5.a, l'article 8, paragraphe 4, et l'article 9, paragraphe 5, autorisent la prise de mesures procédurales supplémentaires pour fournir des garanties supplémentaires ou respecter la législation interne. Les déclarations ne sont pas destinées à être réciproques. Ainsi, par exemple, si une Partie fait une déclaration en vertu de l'article 10, paragraphe 9 – tendant à ce que les demandes soumises en application de cet article ne soient adressées qu'à son autorité centrale –, les autres Parties doivent adresser les demandes à l'autorité centrale de la Partie ayant fait la déclaration, mais cette dernière n'a pas besoin d'adresser les demandes aux autorités centrales des autres Parties, à moins qu'elles ne fassent elles aussi une déclaration en ce sens.

315. Les déclarations visées au paragraphe 2 doivent être faites au moment de la signature par une Partie ou lorsque celle-ci dépose son instrument de ratification, d'acceptation ou d'approbation. En revanche, les déclarations visées au paragraphe 3 peuvent être faites à tout moment.

316. Le paragraphe 3 fait obligation aux Parties de notifier au Secrétaire général du Conseil de l'Europe toute déclaration, notification ou communication visée à l'article 7, paragraphe 5.a et e., et à l'article 8, paragraphes 4 et 10.a et b, du présent Protocole conformément aux conditions spécifiées dans ces articles. Ainsi, par exemple, en vertu de l'article 7, paragraphe 5.e, une « Partie doit, au moment où la notification prévue au paragraphe 5 a est adressée pour la première fois au Secrétaire général du Conseil de l'Europe, communiquer à ce dernier les coordonnées de cette autorité. » De plus, les Parties communiquent au Secrétaire général du Conseil de l'Europe les « autorités » visées à l'article 8, paragraphe 10 a et b. Il a été demandé au Secrétaire général de créer et de tenir à jour un registre de ces autorités désignées par les Parties, et il est demandé à celles-ci de veiller à l'exactitude des informations qui y sont consignées. (Voir l'article 7, paragraphe 5.f, et l'article 8, paragraphe 12).

Article 20 – Statut et retrait des réserves

317. Comme l'article 43 de la Convention, le présent article, sans imposer de délais spécifiques, exige des Parties qu'elles retirent leurs réserves dès que les circonstances le permettent. Afin de pouvoir exercer une certaine pression sur les Parties en vue de les amener au moins à envisager de retirer leurs réserves, le paragraphe 2 autorise le Secrétaire général du Conseil de l'Europe à s'enquérir périodiquement des perspectives de retrait desdites réserves. Cette possibilité de demander des renseignements, devenue pratique courante dans le cadre de l'application de plusieurs instruments du Conseil de l'Europe, se retrouve à l'article 43, paragraphe 3, de la Convention et à l'article 13, paragraphe 2, du Premier Protocole. Les Parties peuvent ainsi indiquer si elles doivent maintenir leurs réserves au sujet de certaines dispositions et retirer ultérieurement celles qui sont devenues inutiles. On espère qu'avec le temps, les Parties pourront retirer autant de réserves que possible de façon à promouvoir l'application uniforme du présent Protocole.

Article 21 – Amendements

318. Le présent article suit la même procédure que celle que prévoit l'article 44 de la Convention pour les amendements. Cette procédure simplifiée permet, en cas de besoin, d'apporter des amendements sans avoir à négocier un protocole d'amendement. Il est entendu que les consultations prévues au paragraphe 3 du présent article ont un caractère non contraignant. Comme indiqué au paragraphe 323 du rapport explicatif de la Convention, « (o)n considère que la procédure d'amendement s'applique pour l'essentiel à des modifications relativement mineures à caractère procédural ou technique. »

Article 22 – Règlement des différends

319. L'article 22 de la Convention s'applique également au présent Protocole (voir le paragraphe 326 du rapport explicatif de la Convention).

Article 23 – Concertation des Parties et évaluation de l'application

320. Le paragraphe 1 du présent article prévoit que l'article 46 de la Convention (Concertation des Parties) est applicable au présent Protocole. Conformément au paragraphe 327 du rapport explicatif de la Convention, l'article 46 a institué « un cadre devant permettre aux Parties de se concerter au sujet de la mise en œuvre de la Convention, des répercussions des nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique ou en relation avec l'ordinateur, et de la collecte de preuves sous forme électronique, ainsi que de l'éventualité de compléter ou d'amender la Convention. » La procédure a été conçue pour être souple: il appartient aux Parties de décider comment ou quand se rencontrer. Après l'entrée en vigueur de la Convention en 2004, les Parties ont commencé à se rencontrer régulièrement dans le cadre du « Comité de la Convention sur la cybercriminalité » (T-CY). Au fil du temps, le T-CY, créé en application de l'article 46 et se conformant au règlement intérieur arrêté par les Parties, a procédé à des évaluations de l'application de la Convention par les Parties, adopté des notes d'orientation devant favoriser une interprétation commune par les Parties des modalités d'application de la Convention et élaboré le projet du présent Protocole. Les procédures à suivre au titre de la concertation des Parties conservent leur souplesse et peuvent donc être adaptées par celles-ci, s'il y a lieu, pour tenir compte de besoins que l'application du présent Protocole pourrait faire apparaître.

321. Comme pour la Convention (voir Rapport explicatif, paragraphe 327), les consultations prévues à l'article 23 devraient " examiner les questions qui se sont posées lors de l'utilisation et de la mise en œuvre de la Convention, y compris les effets des déclarations et réserves formulées ". Cela pourrait inclure des consultations et une évaluation de la mise en œuvre du Protocole par les États constitutifs ou les entités territoriales similaires des États fédéraux notifiés au Secrétaire général du Conseil de l'Europe en vertu de l'article 17, paragraphe 2, et, pour les Parties qui sont membres de l'UE, l'information et la consultation des autres Parties au Protocole sur la législation

de l'UE applicable à l'utilisation et à la mise en œuvre du Protocole en vertu de l'article 15, paragraphe 1.b et 1.c. Outre les consultations par le biais du T-CY en vertu de cet article, examinées dans le paragraphe suivant, les Parties peuvent engager des consultations sur une base bilatérale. Pour les États fédéraux, ces consultations et évaluations se dérouleraient par l'intermédiaire de leur gouvernement central.

322. Le paragraphe 2 dispose établit des procédures spécifiques pour examiner l'utilisation et la mise en œuvre du Protocole dans le cadre plus large établi par l'Article 46 et le T-CY mentionné ci-dessus. Le paragraphe 2 prévoit que « les Parties évaluent périodiquement l'utilisation et la mise en oeuvre effectives des dispositions du présent Porotocole » et indique que l'article 2 du Règlement intérieur établi par le T-CY, tel que révisé le 16 octobre 2020, régira ces évaluations. Ces procédures sont disponibles sur le site web du T-CY. Puisque le T-CY a examiné plusieurs dispositions de la Convention et a publié des rapports conformément à ces procédures, les rédacteurs ont considéré que ces procédures bien établies s'appliquent, *mutatis mutandis*, à l'évaluation des dispositions du présent Protocole. Compte tenu des obligations supplémentaires contractées par les parties à ce protocole et des mesures de coopération uniques qu'il prévoit, les rédacteurs ont décidé que seules les parties au protocole procéderaient à ces évaluations. Compte tenu de l'expertise nécessaire à l'évaluation de l'utilisation et de la mise en œuvre de certaines dispositions du présent Protocole, notamment de l'article 14 sur la protection des données, les Parties peuvent envisager d'associer leurs experts en la matière aux évaluations.

323. Les règles régissant ces évaluations doivent certes être prévisibles, mais l'expérience concrète peut imposer d'adapter ces procédures, sans que soit requis un amendement formel du présent Protocole en vertu de l'article 21. En conséquence, le paragraphe 2 indique que les Parties réexaminent et peuvent modifier ces procédures par consensus cinq ans après l'entrée en vigueur de l'instrument.

324. Étant donné l'importance des garanties de l'article 14, les rédacteurs ont été d'avis que le présent article doit être évalué dès que le niveau de coopération atteint dans le cadre du présent Protocole permet d'examiner utilement l'usage et la mise en œuvre de cette disposition. C'est pourquoi le paragraphe 3 dispose que l'évaluation du présent article commencera une fois que 10 États auront exprimé leur consentement à être liés par ce Protocol.

Article 24 – Dénonciation

325. Les paragraphes 1 et 2 de l'article 24 sont similaires à ceux du paragraphe 47 de la Convention et ne nécessitent aucune explication supplémentaire. Le paragraphe 3 stipule que «[L]a dénonciation de la Convention par une Partie au présent Protocole constitue une dénonciation du présent Protocole». Étant donné que le présent Protocole met l'accent sur le partage d'informations ou de preuves pouvant inclure des données à caractère personnel, les rédacteurs ont jugé prudent d'ajouter le paragraphe 4 pour préciser que «[L]es informations ou preuves transférées avant la date effective de la dénonciation continueront d'être traitées conformément au présent Protocole.