Strasbourg, version 10 novembre 2020 T-CY (2018)23FR rev

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

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

Texte provisoire des dispositions :

- **Langue**
- **Vidéoconférence**
- **Équipes communes d'enquête et enquêtes communes**
- **Divulgation directe de données relatives aux abonnés**
- **Donner effet aux injonctions ordonnant la production accélérée de données**
- **Demande d'informations concernant l'enregistrement d'un nom de domaine (NOUVEAU)**
- **Divulgation accélérée de données informatiques stockées en situation d'urgence (NOUVEAU)**
- **Demandes d'entraide judiciaire urgentes**

Table des matières

1 Langue 3

1.1 Projet de texte 3

1.2 Projet de rapport explicatif 3

2 Utilisation de la vidéoconférence 6

2.1 Projet de texte 6

2.2 Projet de rapport explicatif 7

3 Équipes communes d'enquête et enquêtes communes 11

3.1 Projet de texte 11

3.2 Projet de rapport explicatif 12

4 Divulgation directe de données relatives aux abonnés 16

4.1 Projet de texte 16

4.2 Projet de rapport explicatif 18

5 Donner effet à une injonction d'une autre Partie ordonnant la production accélérée de données 26

5.1 Projet de texte 26

5.2 Projet de rapport explicatif 28

6 Demande d'informations concernant l'enregistrement d'un nom de domaine . 34

6.1 Projet de texte 34

6.2 Projet de rapport explicatif 35

7 Divulgation accélérée de données informatiques stockées en situation d'urgence 39

7.1 Projet de texte 39

7.2 Projet de rapport explicatif 40

8 Demande d'entraide urgente 45

8.1 Projet de texte 45

8.2 Projet de rapport explicatif 46

Contact

Council of Europe
Cybercrime Division
Strasbourg, France
cybercrime@coe.int

1 Langue[1]

1.1 Projet de texte

Article [ ] - Langue

1 Les demandes ainsi que 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 [divulgation directe], ou être accompagnés d'une traduction dans cette langue.

2 Aux fins des articles [divulgation directe], [conservation] et [divulgation d'urgence], une injonction [ou une demande][2] et les renseignements[3] qui l'accompagnent, présentés directement à un fournisseur de services sur le territoire d'une autre Partie, seront :

a. rédigés dans une langue de l'autre Partie dans laquelle le prestataire de services les accepte dans le cadre d'une procédure national comparable ;
b. rédigés dans une autre langue acceptable pour le fournisseur de services ; ou
c. accompagnés d'une traduction dans l'une des langues visées aux alinéas a) ou b).

1.2 Projet de rapport explicatif

1. Cet article fournit un cadre pour les langues qui peuvent être utilisées lorsqu'on s'adresse aux Parties et aux fournisseurs de services. 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.

2. Les traductions inexactes ou coûteuses des demandes d'entraide en matière de criminalité électronique 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 [ ], ou demande de donner effet à une injonction en vertu de l'article [ ]. 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 un protocole.

3. 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 pays. Toutefois, le coût et la difficulté des traductions incombent de manière disproportionnée aux Parties requérantes où des langues moins courantes sont parlées.

4. En raison de cette charge disproportionnée, un certain nombre de pays non anglophones ont demandé que l'anglais soit obligatoire dans un 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

[1] **Texte révisé** tel qu'approuvé provisoirement par le PDP, Strasbourg, 8 Novembre 2019. Le Texte peut changer à mesure que le Protocole évolue et que des commentaires sont reçus.
[2] Revoir plus tard : par exemple, le processus de préservation, etc.
[3] dans la disposition sur la divulgation directe aux « renseignements à l'appui » par opposition aux « renseignements supplémentaires ».

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 les demandes de préservation et, en particulier, les demandes d'urgence au titre du présent Protocole, en anglais ou dans une langue commune plutôt qu'en traduction.

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

6. 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 [divulgation directe] ». 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.

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

a. en vertu de l'article [endossement], de 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 [direct], l'injonction, les renseignements à l'appui et le résumé (paragraphe 5.a).

Le terme « demandes » renvoie également au contenu des demandes d'entraide judiciaire en vertu des articles [entraide judiciaire d'urgence], [vidéoconférence] et [], qui comprend la documentation qui fait partie de la demande.

8. 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 au deuxième Protocole.

9. 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.

10. 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 [direct] » 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.

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

12. Le paragraphe 2 se limite à déterminer la (les) langue(s) que la Partie émettrice utilisera pour soumettre des injonctions [ou des demandes] et les renseignements connexes aux fournisseurs de services. Il précise la ou les langues dans lesquelles une Partie doit présenter une injonction [ou une demande] directement à un fournisseur de services sur le territoire d'une autre Partie aux fins des articles [direct], [conservation] et [divulgation d'urgence]. Il offre des options pour déterminer la ou les langues dans lesquelles l'État requérant peut soumettre une injonction [ou une demande] à un prestataire de services sur le territoire d'une autre Partie. Cette disposition vise à assurer une coopération rapide et une certitude accrue sans imposer une charge supplémentaire aux fournisseurs de services lorsqu'ils reçoivent des injonctions [ou des demandes] de divulguer [ou de conserver] des données. La première option indique que l'injonction [ou la demande] peut être présentée dans une langue dans laquelle le prestataire de services accepte habituellement des injonctions [ou demandes] nationales de ses propres autorités dans le cadre d'enquêtes 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 indique que si un prestataire de services accepte de recevoir des injonctions 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, lorsque l'injonction et les informations qui l'accompagnent ne sont pas rédigées dans l'une de ces langues, elles doivent être accompagnées d'une traduction dans l'une de ces langues.

13. Au paragraphe 2, les termes « injonctions [et demandes] et renseignements complémentaires » désignent l'injonction (paragraphe 3) et les renseignements complémentaires (paragraphe 4) visés à l'article [direct][4].

14. Lorsqu'une Partie a exigé une notification conformément à l'article [direct], 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.

15. Le T-CY s'efforcera également de recueillir de manière informelle des informations sur les langues dans lesquelles les [demandes et] injonctions et les informations qui les accompagnent seront adressées aux prestataires de services en vertu du paragraphe 2 de l'article et en informera les Parties dans le cadre de l'enquête décrite au paragraphe [7] du Rapport explicatif, ci-dessus.

[4] Cette disposition devra peut-être être modifiée si des articles sur la préservation et la divulgation d'urgence sont inclus dans le Protocole.

2 Utilisation de la vidéoconférence

2.1 Projet de texte

Article [ ] – Utilisation de la 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 respectés ; 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 d'interprétation et de transcription.

2. Une Partie requise fournissant son assistance au titre de cet article prend les mesures nécessaires pour obtenir la présence de la personne dont la déposition est requise. 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 juridiction de la Partie requise à l'endroit, à la date et à l'heure fixées.

3. 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, 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.

4. 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 un faux témoignage ou 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, ou
   b. refuse de témoigner alors que la Partie requise a, conformément à son droit interne, intimé à cette personne de 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 juridiction de 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.

5. a. A 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 d'entraide judiciaire 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 d'entraide sera exécutée.

6. 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.

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

2.2 Projet de rapport explicatif

1. L'article [ ] 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, l'article [ ], comme plusieurs autres articles dans ce 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. Ces articles suivent la même approche que celle adoptée par l'article 27 de la Convention de Budapest.

2. De plus, l'article [ ] a la même portée matérielle que l'article 25 de la Convention de Budapest, autrement dit, il s'applique « aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou afin de recueillir les preuves sous forme électronique d'une infraction pénale. » Comme indiqué au paragraphe 253 du Rapport explicatif de la Convention de Budapest, par « infractions pénales liées à des systèmes et des données informatiques », il convient d'entendre « les infractions visées à l'article 14, paragraphe 2, alinéas a-b » de la Convention de Budapest, autrement dit « les infractions pénales établies conformément aux articles 2 à 11 de ladite Convention » et « d'autres infractions pénales commises au moyen d'un système informatique … ».

3. 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. Ainsi, s'il serait plus efficace d'utiliser d'autres méthodes pour exécuter la demande, par exemple par voie écrite avec authentification de registres officiels ou commerciaux, la Partie requise peut choisir d'exécuter la demande par cette autre voie.

4. 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.

5. 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 sauvegardes spécifiques concernant les témoins menacés, les enfants témoins, etc. Ces questions devraient être étudiées et approuvées 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, il est conseillé d'aborder à l'avance 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.

6. 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 2, 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 droit interne de la Partie requise ; la question peut également se poser du degré de confiance à accorder à la comparution volontaire de la personne au moment prévu. En revanche, pour garantir la comparution de la personne, il peut être souhaitable que la Partie requise délivre une injonction ou une citation à comparaître, et ce paragraphe l'y autorise, conformément aux garanties prévues par son droit interne.

7. La procédure pour mener les vidéoconférences est exposée au paragraphe 3. 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.

8. Le paragraphe 4, 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.

9. Le paragraphe 5 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 sous-paragraphe (b) de ce Paragraphe, 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.

10. Si le paragraphe 1 autorise expressément l'utilisation de la technologie de vidéoconférence pour le recueil d'une déposition, l'alinéa (a) du paragraphe 6 prévoit que les dispositions de l'article [ ] peuvent sur consentement mutuel être appliquées aux fins de la réalisation d'une vidéoconférence. De plus, l'alinéa (b) du paragraphe 6 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.

11. Le paragraphe 7 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 7 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 sauvegardes en complément de celles qui s'appliqueraient par ailleurs.

3 Équipes communes d'enquête et enquêtes communes[5]

3.1 Projet de texte

Article [ ] – 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 ; 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.

3. Les autorités compétentes et les autorités participantes communiquent directement entre elles, mais les Parties peuvent convenir d'autres canaux de communication appropriés lorsque des circonstances exceptionnelles nécessitent une coordination plus centrale.

4. 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 Partie concernée sur son territoire aux mêmes conditions que celles s'appliquant en droit interne à une enquête nationale.

5. 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 et droits 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 en notifier sans retard indu les autorités qui ont fourni les informations ou preuves ; ou

[5] Texte tel qu'approuvé provisoirement par le PDP via la procédure écrite, Strasbourg, 15 mai 2020. Le texte peut être modifié en fonction de l'évolution du protocole et des commentaires reçus.

c. pour leur permettre de prévenir une situation de risque significatif et imminent mettant en cause la vie ou la sécurité d'une personne physique[6]. Dans ce cas, les autorités participantes qui ont reçu les informations ou preuves doivent en notifier dans les plus brefs délais les autorités participantes qui les ont fournies, sauf autre accord.

6. 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 [et conformément aux conditions et garanties applicables en droit interne][7].

3.2 Projet de rapport explicatif

1. 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 [.] donne une base pour de telles formes de coopération.

2. 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.

3. Comme indiqué dans l'article [principes généraux concernant ce Chapitre] du présent Protocole et les paragraphes [x à y] 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][8].

Paragraphe 1

4. 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.

5. 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 poursuites pénales à participer à ce type d'accord ; d'autres peuvent autoriser l'autorité centrale – le service normalement responsable des questions d'entraide judiciaire – à le faire. De même, la détermination des autorités qui participent effectivement à une ECE – les "autorités participantes" – relève respectivement des Parties concernées.

[6] La définition/notion de "urgence" devra être harmonisée lorsque d'autres dispositions concernant les situations urgentes (demande d'entraide urgente, [divulgation de contenu en situation urgente]) seront finalisées.
[7] Le texte entre [crochets] sera réexaminé à la lumière de l'approche globale des sauvegardes dans le Protocole.
[8] Note : à réviser une fois que l'article [sur les principes généraux de ce Chapitre] aura été rédigé.

6. [Conformément à l'article 25.2 de la Convention, les Parties au Protocole devraient avoir la capacité de s'engager dans cette forme de coopération [9]].

Paragraphe 2

7. 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 ; le recueil, la transmission et l'utilisation des informations ou preuves ; 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 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 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.

8. Il est supposé que les Parties établiront 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.

9. Les informations ou preuves utilisées dans le cadre de l'équipe commune d'enquête peuvent inclure des données personnelles 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 [garanties] [peut/devrait[10]] s'appliquer au transfert de données personnelles dans le cadre d'ECE.

10. 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

11. En vertu du paragraphe 3, les autorités compétentes déterminées par les Parties en vertu du paragraphe 1 et les autorités participantes visées au paragraphe 3 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 judiciaire peuvent être sollicitées pour aider à se coordonner dans ces circonstances.

[9] Note : ce paragraphe peut être place dans la section plus générale sur l'entraide judiciaire.
[10] Note : il conviendra de retenir "peut" or "devrait" une fois que l'article sur les garanties en matière de protection des données aura été finalisé.

Paragraphe 4

12. Le paragraphe 4 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 effectuerr une mesure d'enquête pour le compte d'une autre Partie sans demande d'entraide.

Paragraphe 5

13. Le paragraphe 5 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 aux alinéas a à c. Les circonstances prévues au paragraphe 5 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 [garanties en matière de protection des données].

14. Il convient de noter que, lorsque les alinéas 5.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.

15. À l'alinéa 5.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.

16. Selon la compréhension des rédacteurs, l'alinéa 5.c fait référence à des circonstances exceptionnelles dans lesquelles les autorités de la Partie destinataire pourraient utiliser directement les informations ou preuves pour prévenir un risque significatif et imminent pour la vie ou la sécurité d'une personne physique. Par « risque pour la sécurité », il est entendu une atteinte grave à l'intégrité physique de la personne. 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 [Para. 2] de l'article [Demandes d'entraide judiciaire urgentes] 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[11]. Si des informations ou preuves sont utilisées en application de l'alinéa 5.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 6

17. 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 6 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 1-2. [Les Parties participant à une enquête conjointe en vertu du paragraphe 6 devraient appliquer les conditions et garanties applicables dans leur droit interne][12].

[11] La définition/notion de "urgence" devra être harmonisée lorsque d'autres dispositions concernant les situations urgentes (demandes d'entraide judiciaire urgentes, [divulgation de contenu en situation urgente]) seront finalisées.
[12] Le texte entre [crochets] sera réexaminé à la lumière de l'approche globale des sauvegardes dans le Protocole.

4 Divulgation directe de données relatives aux abonnés

Note: La Plénière de rédaction du Protocole (ci-après PDP) a adopté provisoirement le texte et le rapport explicatif ci-après, étant entendu qu'ils sont susceptibles d'être modifiés à mesure que les négociations progressent, en fonction des conclusions de l'examen d'autres dispositions qui n'ont pas encore été élaborées et/ou d'autres observations qui pourraient être formulées. En particulier, compte tenu du contexte bien spécifique de la coopération directe entre les autorités et les fournisseurs, une fois que les travaux en cours sur les conditions et les garanties applicables, notamment en matière de protection des données et de respect de la vie privée, auront abouti à un texte et à un rapport explicatif, cet article et son rapport explicatif devraient être examinés par le PDG et la PDP pour déterminer s'il est nécessaire d'apporter des modifications supplémentaires.

4.1 Projet de texte

Article [] : Divulgation 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 ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, 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 [ ], 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. »

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

   a. le nom de l'autorité émettrice et la date d'émission ;
   b. une déclaration indiquant que l'injonction 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, 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. 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 ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, 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 nationales 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 la Partie destinataire ; ou
ii. les conditions ou les motifs de refus visés aux articles 25.4 et 27.4 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 la Partie émettrice aux fins de l'application du paragraphe 5.c ;
ii. doivent informer rapidement la Partie émettrice s'il a été ordonné au fournisseur de services de ne pas divulguer les données demandées et doivent motiver cette décision.

e. Aux fins du paragraphe 5, une Partie doit désigner une autorité unique pour recevoir la communication prévue au paragraphe 5.a et exécuter les tâches liées aux consultations visées aux paragraphes 5.c. et 5.d. La Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les 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. Une Partie peut transmettre l'injonction visée au paragraphe 1, les informations complémentaires visées au paragraphe 4 et la communication visée au paragraphe 5 sous forme électronique. Toutefois, des conditions suffisantes de sécurité et d'authentification peuvent être requises.

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 30 jours suivant sa réception ou dans le délai prévu au sous-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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] 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 déclarer qu'une autre Partie doit solliciter la divulgation de données relatives aux abonnés auprès du fournisseur de services avant de la demander en vertu de l'article [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données], à moins que la Partie émettrice ne fournisse une explication raisonnable justifiant de ne pas l'avoir fait.

9. 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 serait incompatible avec les principes fondamentaux de son ordre juridique interne, se réserver le droit de ne pas appliquer cet article à ces numéros.

4.2 Projet de rapport explicatif

Article [ ] : Divulgation de données relatives aux abonnés

1. 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 Cloud 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 et les procédures pénales, 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.

2. Un nombre croissant d'enquêtes et 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.

3. 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.

4. Les données relatives aux abonnés sont définies à l'article 18.3, selon lequel elles comprennent « 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 » (voir aussi le Rapport explicatif de la Convention sur la cybercriminalité, paragraphes 178-180). 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.

5. Bien que l'article 18 de la Convention de Budapest 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 18.1.a de la Convention) ou « offr[e] des prestations » dans la Partie émettrice (voir article 18.1.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 et aux procédures pénales. 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.

6. Comme indiqué à l'article [Règles générales sur les relations avec la Convention], 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, ni de la mise en place d'une 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 applicables.

Paragraphe 1

7. 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.

8. 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 14(1) de la Convention (voir paragraphes 140 et 152 du Rapport explicatif de la Convention sur la cybercriminalité). 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 18 de la Convention, selon lequel ces dispositions ne peuvent être utilisées pour obtenir la communication de données en masse.

9. Le paragraphe 138 du Rapport explicatif de la Convention de Budapest dispose que le terme « autorités compétentes » désigne une autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de la mesure procédurale. 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.

10. 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

11. Aux termes du paragraphe 2 de l'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 personnelles. 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 [] les garanties requises à cette fin.

12. Comme indiqué au paragraphe 9, le paragraphe 138 du Rapport explicatif de la Convention de Budapest dispose que le terme « autorités compétentes » désigne une autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de la mesure procédurale. La même approche est prévue aux fins de la procédure de coopération directe visée dans ce même article. En conséquence, 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 [8] 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

13. Le paragraphe 3 de l'article précise les informations qui doivent, au minimum, être fournies par une autorité adressant une injonction en application du paragraphe 1 de l'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.

14. En ce qui concerne la différence entre le sous-paragraphe a. (l'autorité émettrice) et le sous-paragraphe e. (l'autorité qui sollicite les données relatives aux abonnés), dans certains pays, 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.

15. 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

16. Alors que le paragraphe 3 énonce les informations qui doivent, au minimum, être transmises lors de l'émission d'une injonction au titre du paragraphe 1, ces injonctions ne peuvent souvent être exécutées que si le fournisseur de services (et, le cas échéant, l'autorité désignée par la Partie destinataire en application du paragraphe 5) reçoit des informations complémentaires. Par conséquent, le paragraphe 4 de l'article 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.

17. 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.

Paragraphe 5

18. Aux termes du paragraphe 5.a, une Partie peut notifier au Secrétaire Général du Conseil de l'Europe que, lorsqu'elle se trouve être la Partie destinataire, elle exige de la Partie émettrice qu'elle l'informe simultanément de l'émission de toute injonction adressée directement à un fournisseur de services sur son territoire, dans chaque cas (c'est-à-dire pour toutes les injonctions adressées aux fournisseurs sur son territoire) ou dans certaines circonstances déterminées.

19. 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 destinataire.

20. 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.

21. Les Parties destinataires 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 [18 du Rapport explicatif de l'article [Exécution]]. De ce fait, la possibilité pour une Partie d'être informée ou consultée constitue une garantie supplémentaire. Cela dit, la coopération doit en principe être étendue et les entraves dont elle peut faire l'objet doivent être strictement limitées. En conséquence, les conditions et les refus devraient également être limités, conformément aux objectifs de cet article, qui sont d'éliminer les obstacles à l'accès transfrontalier aux éléments de preuve électroniques aux fins d'enquêtes pénales et de prévoir des procédures plus efficaces et plus rapides en ce sens.

22. La mise en œuvre de cet article – y compris de la mesure dans laquelle une Partie devrait pouvoir invoquer des motifs de refus – est affectée par d'autres dispositions, comme le champ d'application, les conditions et les garanties (notamment en matière de protection des données). Le dispositif et le rapport explicatif relatifs à ces autres articles présentent en détail la manière dont cet article est concerné.

23. 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 émettrice 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. Les autorités de la Partie destinataire doivent recueillir les informations nécessaires et prendre leur décision « dans les plus brefs délais ». Ils doivent également informer rapidement les autorités de la Partie émettrice s'ils décident d'ordonner au fournisseur de services de ne pas répondre favorablement, en indiquant les raisons de cette décision.

24. 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.

25. Aux termes du paragraphe 5.e, une Partie qui exige d'être informée ou consultée doit désigner une autorité unique et communiquer au Secrétaire Général du Conseil de l'Europe les coordonnées de cette autorité.

26. Une Partie peut modifier son exigence de notification 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.

27. 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 et des autorités consultées par les fournisseurs en application du paragraphe 5.b. 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 et de consultation 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 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

28. Le paragraphe 6 indique clairement que la transmission d'une injonction ou la communication d'informations à une autre Partie par voie électronique, y compris par l'utilisation de courrier électronique et de portails électroniques, est autorisée. L'objectif est d'encourager le recours à des moyens électroniques lorsque la loi ne l'interdit pas, 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 3 de l'article [Entraide judiciaire d'urgence] et d'autres orientations concernant les exigences en matière de sécurité sont proposées au paragraphe [ ] du Rapport explicatif. L'article [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] contient également des dispositions similaires, au paragraphe 5.

Paragraphe 7

29. 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] ou d'une autre forme d'entraide. Les Parties qui invoquent cet article ne peuvent chercher à obtenir une exécution unilatérale.

30. S'agissant de l'exécution de l'injonction au moyen de l'article [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données], 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] afin qu'il soit plus facile, pour la Partie émettrice, d'obtenir des données relatives aux abonnés.

31. 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données]. 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.

32. 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] 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 [Exécution] ou de tout autre mécanisme d'entraide qui pourrait donner lieu à un refus.

Paragraphe 8

33. 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données], 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] et, par conséquent, pourraient réduire le nombre de cas dans lesquels l'article [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] doit être invoqué. Les procédures prévues par l'article [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] 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 [Exécution des injonctions adressées par une autre Partie en vue d'une divulgation rapide des données] 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

34. 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.

35. Le paragraphe 9.b dispose que – pour les raisons mentionnées au paragraphe [4] 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.

5 Donner effet à une injonction d'une autre Partie ordonnant la production accélérée de données

Note: La PRP a adopté provisoirement le texte suivant et son rapport explicatif, étant entendu que ces derniers peuvent évoluer à mesure des négociations, en fonction des décisions prises concernant d'autres dispositions qui n'ont pas encore été préparées et/ou d'autres observations reçues. En particulier, une fois que les travaux en cours sur les conditions et les sauvegardes en matière de protection des données et de vie privée auront abouti à un texte et un rapport explicatif, le présent article et son rapport explicatif devraient être examinés par le PDG et la PRP afin de déterminer si d'autres changements sont nécessaires.

5.1 Projet de texte

Article [ ] : Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données

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 (la Partie requise) 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,
   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 criminelles spécifiques menées par la Partie requérante.

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour donner effet aux injonctions de production visées au paragraphe 1 qui sont soumises par une autre Partie (Partie requérante).

3. 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 :

      i. spécifie l'autorité émettrice et la date d'émission ;
      ii. contient une déclaration selon laquelle l'injonction est soumise en vertu du présent protocole ;
      iii. spécifie le nom et l'adresse du ou des fournisseurs de services à laquelle elle doit être notifiée ;
      iv. indique la ou les infractions objet de l'enquête ou des poursuites pénales ;
      v. précise l'autorité à l'origine de la demande de données, si elle est différente de l'autorité ayant délivré l'injonction ; et
      vi. décrit de manière détaillée des 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 sans le consentement de la Partie requérante spécifient :

      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 données a déjà été demandée, auquel cas le document précisera la date de la demande et la cote de référence ;
viii. si 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, d'adoption ou d'adhésion, 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 45 jours au plus en lui ordonnant de produire les informations en retour dans les :

i. 20 jours pour des informations relatives à l'abonné, et
ii. 45 jours pour les données relatives au trafic.

b. La Partie requise procède sans retard 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 25.4 ou à l'article 27.4 de la Convention pour refuser l'exécution d'une demande ou soumettre cette exécution à des conditions. Elle peut invoquer les raisons visées à l'article 27.5 pour ajourner l'exécution d'une demande. Dans tous les cas, 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.

9. Au moment de la signature ou lors du dépôt de son instrument de ratification, d'acceptation, d'accord ou d'adhésion, chaque Partie communique au ou à la Secrétaire Générale 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.

10. Une Partie peut, au moment de la signature ou lors du dépôt de son instrument de ratification, d'acceptation, d'accord ou d'adhésion, 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 autorité désignée d'un commun accord entre les Parties concernées.

11. 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 9. Chaque Partie veille à ce que les coordonnées portées au registre soient en permanence correctes.

12. Une Partie peut se réserver le droit de ne pas appliquer le présent article aux données relatives au trafic.

5.2 Projet de rapport explicatif

Article [ ] Donner effet aux injonctions d'une autre Partie ordonnant la production urgente de données

1. Cet article a pour but de donner à une Partie requérante la capacité d'émettre une injonction à produire à une Partie requise 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.

2. L'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.

3. 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.

4. La notion d' « autorité compétente » aux fins de la Convention est analysée dans le Rapport explicatif de la Convention (au paragraphe 138), cependant elle n'est pas définie dans la Convention elle-même. Dans le droit fil des explications fournies au paragraphe 138 du Rapport explicatif de la Convention, 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 procédurales 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 9 du présent article, comme décrit de manière plus détaillée ci-dessous.

5. 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.

6. En vertu du paragraphe 2, la Partie requise doit donner effet sur son territoire à une injonction émise en vertu du paragraphe 1, sous réserve des sauvegardes 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 sauvegardes supplémentaires, y compris celles qui sont nécessaires en matière de production des données relatives au trafic.

7. Il existe certes diverses manières d'appliquer l'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.

8. 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 l'alinéa 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 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 de l'alinéa 3.b peuvent être partagées avec le fournisseur de services. En vertu de l'alinéa 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 en vertu de l'article 27.8 de la Convention.

9. L'injonction de produire des informations concernant l'abonné ou de données concernant le trafic décrite à l'alinéa 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 (article 18.3 de la Convention de Budapest) ; 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 (article 1.d de la Convention de Budapest)), 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.

10. 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.5, 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 à l'alinéa 1 de l'article sont remplies, autrement dit si les informations ou données sont « nécessaires pour les enquêtes ou procédures 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 désignée 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 la préservation soit prorogée 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.

11. 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.

12. 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.

13. 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.

14. En vertu du paragraphe 4, il peut être nécessaire de fournir des informations complémentaires à la Partie requise pour donner effet à l'injonction. Ainsi, dans le droit interne de certaines Parties, la production de données sur le trafic peut exiger la communication d'informations supplémentaires du fait de conditions supplémentaires dans ce droit pour l'obtention de ces données. De plus, la Partie requise peut demander des éclaircissements concernant les informations fournies en vertu 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.

15. Le paragraphe 5 a pour but d'encourager les Parties à recourir à des moyens de communication électronique sécurisés et authentifiables pour faciliter la transmission d'information ou de données et documents, y compris pour la transmission des injonctions et informations à l'appui de ces dernières, et pour l'envoi des informations ou données et documents produits (voir paragraphe 4 du Rapport explicatif concernant l'entraide judiciaire d'urgence).

16. En vertu du paragraphe 6, la Partie requise devrait prendre les mesures raisonnables 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. Les Parties devraient 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 ce qui est raisonnablement en leur pouvoir pour mener à bien uniquement les processus sous leur contrôle.

17. 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.

18. En vertu du paragraphe 8, la Partie requise peut refuser de donner suite à une partie du processus qui donne effet à l'injonction de la Partie requérante, ou déterminer qu'une partie de l'injonction seulement peut se voir donner effet en fonction des circonstances en l'espèce, ou encore refuser l'intégralité de la demande en présence des motifs de refus établis aux articles 25.4 ou 27.4 de la Convention. En outre, la Partie requise peut surseoir à l'exécution de l'injonction en vertu de l'article 27.5 de la Convention. La Partie requise notifie la Partie requérante de sa décision de refus ou de sursis de l'exécution de toute partie de la demande.

19. L'application de cet article – y compris la mesure dans laquelle une Partie devrait pouvoir s'appuyer sur les motifs de refus – est affectée par d'autres dispositions, par exemple le champ d'application ainsi que les conditions et sauvegardes (y compris pour ce qui est de la protection des données). Le texte opératoire et le rapport explicatif concernant d'autres articles de cette nature détaillent la manière dont le présent article est affecté.

20. Il convient de rappeler que le paragraphe 253 du Rapport explicatif de la Convention de Budapest 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.

21. Le paragraphe 9 a pour but de faire en sorte que les Parties, au moment de la signature ou lors du dépôt de leurs instruments de ratification, d'acceptation, d'adoption ou d'adhésion, identifient les autorités charges de soumettre et de recevoir des injonctions en vertu de cet article. Les Parties n'ont pas besoin d'indiquer le nom et l'adresse d'une personne donnée mais peuvent préciser qu'un bureau ou service a été jugé compètent aux fins de l'envoi et de la réception d'injonctions en vertu de cet article.

22. Le paragraphe 10 permet à une Partie de déclarer qu'elle demande que les injonctions qui lui sont soumises en vertu de cet article soient transmises par une autorité centrale de la Partie requérante ou une autre autorité s'il en est ainsi convenu entre les Parties. Toute(s) autorité(s) centrale(s) désignée(s) par la Partie requérante en vertu de l'article 27.2.a de la Convention peut ou peuvent transmettre une telle injonction. Les Parties sont encouragées à prévoir la plus grande souplesse pour la soumission de demandes.

23. Le paragraphe 11 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 9 et que chaque Partie veille à ce que les informations contenues dans le registre soient justes et précises. Ces informations aideront les Parties requises à vérifier l'authenticité des demandes.

24. En vertu du paragraphe 12, 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.

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

Note: La PRP a adopté provisoirement le texte suivant et son rapport explicatif le 9 novembre 2020, étant entendu que ces derniers peuvent évoluer à mesure des négociations, en fonction des décisions prises concernant d'autres dispositions qui n'ont pas encore été préparées et/ou d'autres observations reçues. En particulier, une fois que les travaux en cours sur les conditions et les sauvegardes en matière de protection des données et de vie privée auront abouti à un texte et un rapport explicatif, le présent article et son rapport explicatif devraient être examinés par le PDG et la PRP afin de déterminer si d'autres changements sont nécessaires.

6.1 Projet de texte

Article [ ] : 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[13],] à émettre auprès d'une entité fournissant des services 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 le registrant 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 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 ;
   d. le délai et le moyen de divulgation de ces informations et toutes autres instructions procédurales spéciales.

4. [Les informations divulguées en réponse à une demande visée au paragraphe 1 sont soumises aux garanties appropriées conformément aux articles 15 et [protection des données].][14]

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 ce qu'il est possible de faire pour obtenir les informations.

[13] Ceci pourrait faire partie d'une disposition générique : rester cohérent avec d'autres articles.
[14] Vérifier s'il faut inclure ce paragraphe dans le contexte d'une revue globale des garanties dans le protocole.

6.2 Projet de rapport explicatif

1. Cet article établit une procédure qui prévoit la coopération directe entre les autorités d'une Partie et une entité prestataire de services concernant des noms de domaine située sur le territoire d'une autre Partie pur obtenir des informations sur l'enregistrement de noms de domaine sur Internet. Comme pour l'article [divulgation d'informations relatives à l'abonné], la procédure s'appuie sur les conclusions du Groupe du Comité de la Convention chargé des preuves dans le Cloud, reconnaissant l'importance que revêt un accès transfrontière rapide à des preuves électroniques pour des enquêtes et procédures pénales, au vu des difficultés que posent les procédures existantes pour l'obtention de preuves électroniques.

2. La procédure reconnaît également le modèle actuel de gouvernance de l'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 du Deuxième protocole additionnel, autrement dit des enquêtes et 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[2].

3. 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 « registrant ») est donc critique pour identifier un suspect dans une enquête ou procédure pénale spécifiques. 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.

4. Les informations concernant l'enregistrement de noms de domaine sont détenues par des entités prestataires de services concernant des 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 personnelles 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 concernant des noms de domaines (registraire ou registre) ou la personne à laquelle se réfèrent les données.

5. L'article [Demande d'informations concernant l'enregistrement d'un nom de domaine] 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 de l'Internet.

Paragraphe 1

6. 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 concernant des noms de domaines 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 juridique interne, 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.

7. 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.

8. Comme prévu dans l'article [Dispositions de portée générale] du présent Protocole, une demande en vertu du paragraphe 1 peut être émise uniquement aux fins d'enquêtes et procédures pénales spécifiques. De plus, l'expression « autorités compétentes » est à prendre dans le même sens que pour le paragraphe 138 du Rapport explicatif de la Convention en ce qu'elle « désigne une autorité judiciaire, administrative ou policière habilitée en droit interne à ordonner, autoriser ou entreprendre l'exécution de procédures de collecte ou de production d'éléments de preuve se rapportant à des enquêtes ou procédures pénales ». Une « entité prestataire de services concernant des 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 concernant des noms de domaine ».

9. Si les informations pour identifier ou contacter le registrant d'un nom de domaine sont souvent stockées par des entités prestataires de services génériques 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 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 des noms de domaine – ou les futurs types de services de ce genre – peuvent être utilisés pour perpétrer des actes de cybercriminalité.

10. 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 nom 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

11. Le paragraphe 2 fait obligation à chaque Partie d'adopter des mesures pour permettre à des entités prestataires de services établies sur son territoire concernant des noms de domaine de divulguer ces informations en réponse à une demande visée au paragraphe 1, sous réserve des conditions raisonnables prévues par le droit interne. Ces mesures devraient faciliter la divulgation des données demandées de manière rapide et efficace dans toute la mesure du possible.

12. Dans le même temps, 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 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 [paragraphes opératives 1 et 3.a et paragraphe ER []];
- le Protocole prévoit qu'une demande est faite aux fins d'enquêtes ou de procédures pénales spécifiques [article dispositions générales];
- 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 [paragraphe opératif 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 [Conditions / garanties];
- 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

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

a. la date d'émission ainsi que l'identité et les coordonnées de l'autorité émettrice (alinéa a.), laquelle doit être une autorité compétente au sens du paragraphe [8] du Rapport explicatif habilitée à émettre de telles demandes en vertu du paragraphe 1 de l'article ;
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 (alinéa 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 (alinéa 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. 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 sur la cybercriminalité). D'autres Parties appliqueront les principes de leur droit interne adaptés tels que le principe de pertinence (en d'autres termes, la preuve recherchée par une demande

doit être pertinente pour l'enquête ou les poursuites. Les parties devraient éviter les demandes générales de divulgation d'informations concernant les noms de domaine, à moins qu'elles ne soient nécessaires pour l'enquête ou la procédure pénale spécifique ;

d. l'échéance et les modalités de divulgation des informations et autres instructions procédurales spéciales (alinéa d.). L'expression "Instructions procédurales spéciales" entend faire référence à 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 concernant des 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.

14. 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

15. Les lois de certaines Parties relatives à la protection des données contenant des dispositions visant à autoriser les transferts internationaux d'informations en réponse à une demande en vertu du présent article, le présent Protocole contient à l'article [ ] des garanties requises à cette fin.]

Paragraphe 5

16. 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.

7 Divulgation accélérée de données informatiques stockées en situation d'urgence

Note: La PRP a adopté provisoirement le texte suivant et son rapport explicatif le 10 novembre 2020, étant entendu que ces derniers peuvent évoluer à mesure des négociations, en fonction des décisions prises concernant d'autres dispositions qui n'ont pas encore été préparées et/ou d'autres observations reçues. En particulier, une fois que les travaux en cours sur les conditions et les sauvegardes en matière de protection des données et de vie privée auront abouti à un texte et un rapport explicatif, le présent article et son rapport explicatif devraient être examinés par le PDG et la PRP afin de déterminer si d'autres changements sont nécessaires.

7.1 Projet de texte

Article [Divulgation rapide de données informatiques stockées en cas d'urgence]

1. a. Chaque Partie adopte les mesures législatives et autres pouvant se révéler nécessaires pour que son Point de contact du Réseau 24/7 visé à l'article 35 de la Convention (« Point de contact ») puisse, en situation d'urgence tel que défini à l'article [Entraide judiciaire en cas d'urgence], transmettre une demande à un Point de contact dans une autre Partie et recevoir directement une demande d'un Point de contact dans une autre Partie 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 déclarer qu'elle n'exécutera pas de demandes introduites en vertu de l'alinéa 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 1.a ; et

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

3. La demande introduite en vertu du paragraphe 1 spécifie :

   a. spécifie l'autorité émettrice et la date d'émission ;
   b. contient une déclaration selon laquelle la demande est émise en vertu du présent Protocole ;
   c. précise le nom et l'adresse du fournisseur de services en possession des données recherchées ou qui en a 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 informations 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. Elle peut exiger des niveaux appropriés de sécurité et d'authentification avant d'accepter la demande.

5. Une Partie peut déclarer qu'elle exige de la Partie requérante que celle-ci, après l'exécution de la demande, lui fournisse 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. Lorsqu'une Partie requise décide qu'elle ne fournira les données demandées à une Partie qui lui en a fait la demande en vertu du paragraphe 1 du présent article, la Partie requise en informe la Partie requérante rapidement et, au besoin, spécifie les éventuelles conditions dans lesquelles elle fournirait les données et toutes autres formes de coopération qui peuvent être utilisées.

7.2 Projet de rapport explicatif

Introduction

1. 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 du Rapport explicatif [entraide judiciaire en situation urgente], il peut être nécessaire de demander une coopération la plus rapide possible dans diverses situations où le facteur temps est fondamental, 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.

2. En vertu de la Convention, dans des situations d'urgence, les Parties font des demandes d'assistance mutuelle pour obtenir des données et, en vertu de l'article 35, paragraphe 1, point 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 judiciaire.

3. Comme indiqué dans l'article [Règles générales relatives à la relation avec la Convention], le présent article ne porte pas atteinte à la coopération (y compris spontanée) entre les Parties ou entre les Parties et les fournisseurs de services par le biais d'autres accords, arrangements, pratiques ou lois nationales applicables. Par conséquent, en vertu du 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 [Entraide judiciaire en situation urgente].

4. 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 le droit interne de la Partie. Ces Points de Contact peuvent également conseiller les Parties requérantes sur des questions qu'elles pourraient se poser concernant les fournisseurs et la collecte de preuves électroniques, par exemple, en expliquant le cadre de droit interne qui doit être satisfait pour obtenir des éléments de preuve. Cette communication en aller-retour améliore la compréhension par la Partie requérante du droit interne dans la Partie requise et permet un recueil plus facile des éléments de preuve nécessaires.

5. L'utilisation du canal prévu au présent article peut avoir des avantages par rapport au canal d'entraide judiciaire d'urgence énoncé à l'article [entraide judiciaire urgente]. 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

6. En vertu de l'alinéa 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 [dispositions générales], la demande doit être présentée dans le cadre d'une enquête ou procédure pénale.

7. 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 comme décrit au paragraphe 5 du RE ci-dessus, sous réserve de la possibilité d'une déclaration au titre de l'alinéa 5 du dispositif. Le terme « urgente » est défini à l'article [entraide judiciaire urgente].[15] En vertu du présent article, la Partie requise déterminera s'il existe une « urgence » par rapport à une demande en utilisant les informations fournies au paragraphe 3.

8. Contrairement à d'autres articles du présent Protocole, tels que l'article [divulgation directe], qui ne peuvent être utilisés que pour obtenir des « informations relatives à l'abonné

[15] Note : La définition/le concept d'"urgence" et le terme "atteinte grave" visés dans cette disposition et dans d'autres dispositions [entraide d'urgence, Équipes communes d'enquête] devront être alignés. À cet égard, le rapport explicatif de l'article [entraide d'urgence] devrait être revu afin de s'assurer que la description des atteintes graves est conforme aux pratiques nationales dans ce domaine.

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. 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 RE de la Convention ER par. 170.)

9. 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.

10. En vertu de l'alinéa 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. 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 [coopération directe] ou [donner effet], 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

11. Le paragraphe 2 exige que chaque Partie adopte les mesures nécessaires pour s'assurer que son cadre juridique national permet à ses autorités de demander et d'obtenir des données demandées en vertu du paragraphe 1 auprès des fournisseurs de services sur son territoire et de 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.

12. 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.

13. 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, dans le cadre de son droit interne, 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

14. 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.

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

16. En ce qui concerne l'alinéa 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 obtenues 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.

17. En application de l'alinéa 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 [Entraide judiciaire urgente], 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 en vertu de son droit interne, elle devrait consulter le Point de Contact du Réseau 24/7 de la Partie requérante.

18. En application de l'alinéa 3.g, la demande précise toute instruction procédurale spéciale. Il s'agit notamment des demandes particulières de non-divulgation de la demande aux abonnés 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 déterminent, en consultation avec les autorités de la Partie requérante, quand et de quelle manière la confirmation de l'authenticité doit être donnée.

19. 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

20. Le paragraphe 4 a pour but d'encourager les Parties à utiliser des moyens de communication rapides pour faciliter la transmission des informations ou données et documents, notamment la transmission des demandes et l'envoi des données produites. Ce paragraphe se fonde sur le paragraphe [] de l'article [donner effet], mais il a été modifié pour ajouter qu'une Partie peut accepter des demandes formulées oralement, méthode de communication fréquemment utilisée par le Réseau des points de contact 24/7.

Paragraphe 5

21. 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 leur droit interne, 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[16].

Paragraphe 6

22. 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 [entraide d'urgence] 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.

[16] Vérifier les déclarations tout le long du Protocole.

8 Demande d'entraide urgente[17]

8.1 Projet de texte

Article [ ] – Demande d'entraide urgente [18, 19]

`

1. Aux fins du présent article, par « situation urgente » il convient d'entendre une situation présentant un risque significatif et imminent pour la vie ou la sécurité d'une personne physique.

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

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

4. La Partie requise peut, en urgence, 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.

5. 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 avec la plus grande célérité.

6. Chaque Partie s'assure qu'une personne de son autorité chargée de répondre aux demandes d'entraide en vertu de l'article 25 ou de l'article 27 de la Convention est disponible vingt-quatre heures sur vingt-quatre sept jours sur sept pour répondre à une demande d'entraide transmise en vertu du présent article.

7. Les 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.

8. a. En cas d'urgence, des demandes d'entraide peuvent être adressées directement par les autorités judiciaires de la Partie requérante à leurs homologues de la Partie requise, ou par le biais d'Interpol ou du point de contact 24/7 établi au titre de l'article 35 de la Convention. Dans ce 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 d'entraide est envoyée directement à une autorité judiciaire de la Partie requise et que ladite autorité n'est pas compétente pour la traiter, cette

[17] Texte tel qu'adopté provisoirement par le PDP, Strasbourg, 11 juillet 2018. Ce texte peut évoluer en fonction de l'évolution du Protocole et des observations qui sont reçues.

[18] ***Ajouter au Protocole :

- Aux fins du présent article, le champ de l'entraide judiciaire sera identique à celui prévu à l'article 25 de la Convention de Budapest.
- Pour plus de certitude, aucune disposition dans cet article n'empêche le partage d'information ou la fourniture d'un autre type d'assistance international par d'autres voies possibles de coopération internationale.

[19] *** Ajouter que cette disposition n'exclut pas d'autres options [autrement dit "Cette disposition n'empêche pas la transmission volontaire de données à des autorités compétentes étrangères par des fournisseurs de services sur Interne en conformité avec les dispositions légales applicables en droit interne et au niveau international. »]

dernière la transfère à l'autorité nationale compétente et en notifie directement la Partie requérante.

b. Chaque Partie peut, au moment de la signature ou lors du dépôt de son instrument de ratification, d'acceptation, d'adoption ou d'adhésion, informer le Secrétaire Général du Conseil de l'Europe que, pour des raisons d'efficience, les demandes d'entraide judiciaire formulées en vertu du présent paragraphe doivent être adressées exclusivement à son autorité centrale.

8.2 Projet de rapport explicatif

1. L'article [ ] du protocole (Demande d'entraide judiciaire urgente) a pour but de prévoir une procédure qui soit la plus rapide possible pour les demandes d'entraide effectuées en situation d'urgence. Le paragraphe 1 définit une situation urgente comme une situation présentant un risque significatif et imminent pour la vie ou la sécurité d'une personne physique. La définition vise à inclure les situations dans lesquelles le risque est imminent ; autrement dit elle ne couvre pas des situations où le risque pour la vie ou la sécurité de la personne physique n'existe plus, ou pourrait exister à l'avenir mais sans être imminent. Si cette définition est très précise, c'est parce qu'elle fait peser sur les Parties requise comme requérante, qui doivent réagir de manière extrêmement plus rapide en cas d'urgence, des obligations mobilisant beaucoup de ressources humaines, les demandes d'entraide urgentes devant, de par leur nature, bénéficier d'un traitement plus prioritaire que d'autres demandes importantes mais qui sont quelque peu moins urgentes, même si elles avaient été soumises antérieurement.

2. Étant donné que l'article [ ] du Protocole est limité aux circonstances justifiant une telle célérité dans l'action, il est distinct de l'article 25(3) de la Convention-mère, 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 dans l'article [ ] du Protocole. En d'autres termes, l'article 25(3) a une portée plus large que l'article [ ] 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(3) prévoit une méthode plus rapide pour transmettre une demande et y répondre, les obligations en cas d'urgence relevant de l'article [ ] du Protocole sont nettement plus lourdes ; en d'autres termes, lorsqu'une demande d'entraide judiciaire est transmise pour prévenir un risque significatif et imminent pour la vie ou la sécurité d'une personne physique, le processus devrait être encore plus rapide. Les urgences impliquant un risque significatif et imminent pour la vie ou la sécurité d'une personne physique concernent souvent des prises d'otages où il y a un risque crédible et imminent que la victime perde la vie, soit gravement blessée ou se voie infliger d'autres dommages et où le suspect négocie une rançon par mail ou via les médias sociaux, de sorte que la localisation de la victime peut être déterminée au moyen de données stockées par le fournisseur ; il peut s'agir aussi d'abus sexuels repérés par la découverte de matériels produits peu de temps avant concernant l'exploitation ou l'abus sexuel d'un enfant ; cela peut concerner également d'autres indices d'abus, des situations post-attentat terroriste où les autorités cherchent à déterminer si d'autres attentats sont imminents, et des menaces à l'encontre de la sécurité d'infrastructures critiques qui présentent un risque significatif et imminent de danger pour la vie ou la sécurité d'une personne physique.

3. En vertu du paragraphe 2, lorsqu'une Partie transmet une demande d'entraide urgente, outre les autres informations devant figurer dans la demande en vertu du traité applicable ou du droit interne de la Partie requise, la Partie requérante doit à la fois conclure qu'il existe une urgence au sens de cet article, 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. A cet égard, il convient de rappeler qu'au titre de l'article 25(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».

4. Le paragraphe 3 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.

5. Lorsque la Partie requise demande un complément d'informations pour étayer la situation urgente au sens du paragraphe 1, et/ou que les autres conditions liées à la demande d'entraide ont été remplies, le paragraphe 4 prévoit que ce complément d'informations doit être demandé aussi rapidement que possible et, réciproquement, exige de la Partie requérante qu'elle communique le complément d'informations avec la même célérité. Il est donc demandé aux deux Parties de faire leur maximum pour éviter toute perte de temps qui pourrait involontairement entraîner une issue tragique.

6. En vertu du paragraphe 5, 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 en faisant au plus vite. 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 l'État requis ne sauraient être tenues responsables des retards occasionnés par les délais de réponse du fournisseur à ces injonctions.

7. En vertu du paragraphe 6, toutes les Parties veillent à ce que des membres de leur autorité centrale chargée de l'entraide (ou, si l'article [ ](8) est applicable, des autorités judiciaires pertinentes concernées) 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 judiciaire. L'obligation prévue dans ce paragraphe n'exige pas de l'autorité responsable de la réponse aux demandes d'entraide judiciaire relevant des articles 25 ou 27 de la Convention qu'elle prévoie un personnel d'astreinte 24/7. 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.

8. Le paragraphe 7 offre une base qui permet aux Parties concernées de s'entendre sur un canal alternatif de transmission de la preuve ou des informations demandées ; 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 preuves ou informations prévues 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 Parties peuvent convenir 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 Parties peuvent aussi, par exemple, convenir d'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 encore s'entendre sur la transmission de preuves sensibles.

9. Enfin, le paragraphe 8 est une version plus concise de l'article 27(9) de la Convention-mère, au titre duquel les Parties au protocole peuvent prévoir que les demandes sont faites directement entre autorités judiciaires. Dans certaines Parties, ce type de canal direct entre autorités

judiciaires est bien établi et peut se révéler efficace pour accélérer encore la création et l'exécution des demandes d'entraide. La transmission de la demande d'entraide urgente par l'intermédiaire du point de contact 24/7 de la Partie ou via Interpol est utile, non seulement parce qu'elle limite les retards mais aussi parce qu'elle permet des normes plus strictes de sécurité et d'authentification. Toutefois, dans certaines Parties, l'envoi d'une demande d'entraide directement à une autorité judiciaire de la Partie requise sans impliquer l'autorité centrale chargée de l'entraide ni obtenir son autorisation pourrait se révéler contreproductif ; en effet, sans conseils et/ou accord de l'autorité centrale, il est possible que l'autorité destinataire de la demande ne soit pas en mesure d'agir seule, ou ne connaisse pas la procédure correcte. En conséquence, comme pour l'article 25(9)e, chaque Partie peut notifier au Secrétaire Général du Conseil de l'Europe que les demandes d'entraide judiciaire introduites en vertu du présent article doivent être adressées exclusivement à son autorité centrale.