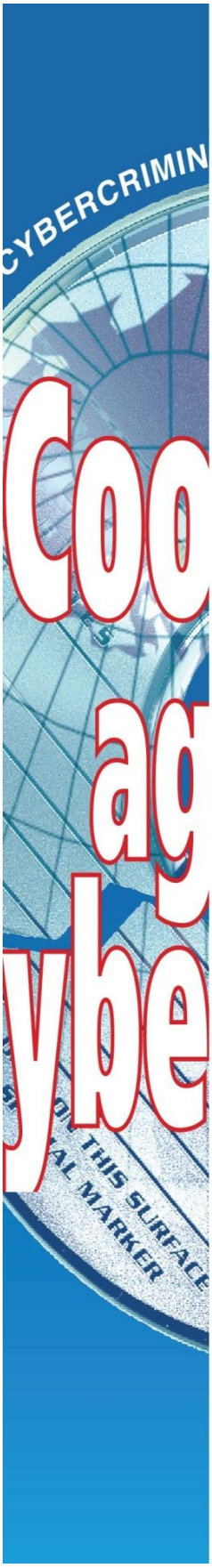

Comité de la Convention sur la cybercriminalité (T-CY)

Rapport d'évaluation

Mise en œuvre des dispositions de la Convention de Budapest en matière de préservation des données

Adopté par le T-CY lors de sa 8e réunion plénière (5-6 décembre 2012)

T-CY (2012)10 REV

Strasbourg, 25 janvier 2013 (provisoire)

www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Table des matières

Contact

Alexander Seger
Secrétaire du Comité de la Convention sur la cybercriminalité (T-CY) Tél. : +33-3-9021-4506
Direction générale Droits de l'homme et Etat de droit Fax : +33-3-9021-5650
Conseil de l'Europe, Strasbourg, France E-mail : alexander.seger@coe.int

Note de la traductrice

Les équivalents français retenus dans les textes officiels pour *expedited preservation* (Convention de Budapest : « conservation rapide ») et *data retention* (directive UE : « conservation des données ») risquaient d'engendrer une grande confusion. C'est pourquoi, dans le présent texte, *expedited preservation* et *data preservation* ont été systématiquement traduits par « préservation rapide » et « préservation des données », y compris dans les citations de la Convention.

1 Introduction

Lors de sa 6e réunion plénière (23-24 novembre 2011), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de « faire le point sur l'application effective de la Convention par les Parties »[1].

Les Parties ont décidé d'examiner en 2012 les dispositions relatives à la préservation rapide :

- Article 16 – Préservation rapide de données informatiques stockées (niveau national)
- Article 17 – Préservation et divulgation rapides de données relatives au trafic (niveau national)
- Article 29 – Préservation rapide de données informatiques stockées (niveau international)
- Article 30 – Divulgation rapide de données conservées

L'objectif de ce rapport est d'améliorer l'application concrète de la Convention de Budapest sur la cybercriminalité en évaluant sa mise en œuvre par les Parties, en identifiant les bonnes pratiques, en aidant à résoudre les problèmes rencontrés et en partageant les expériences des pays qui ont adhéré ou envisagent d'adhérer à la Convention.

Concernant les quatre articles analysés, le rapport devrait

- expliciter la différence entre le concept de préservation rapide (articles 16, 17, 29 et 30) et celui de conservation des données (non prévu par la Convention de Budapest mais appliqué dans de nombreux pays, notamment en vertu de la directive européenne sur la conservation des données) ;
- encourager l'utilisation concrète des dispositions en matière de préservation dans les enquêtes nationales et internationales ;
- promouvoir un plus grand rôle du Réseau 24/7 dans l'obtention de preuves électroniques au niveau international.

Un questionnaire, préparé par le Bureau du T-CY en janvier 2012, a été envoyé aux représentants du T-CY le 15 février 2012, avec copie aux représentations permanentes[2].

Lors de sa 7e réunion plénière (4 et 5 juin 2012), le T-CY a examiné une première version du présent rapport d'évaluation et adopté des conclusions préliminaires[3]. Il a été décidé d'achever l'évaluation des quatre dispositions lors de la 8e réunion plénière, en décembre 2012.

A sa 8e réunion plénière, le T-CY a adopté le rapport d'évaluation en principe, dans l'attente d'informations supplémentaires à fournir par certaines Parties.

Le rapport définitif a été adopté par le T-CY le 25 janvier 2013, au terme d'une procédure écrite.

---

[1] Objectif n° 3 du Plan de travail pour la période janvier 2012-décembre 2013.
http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY_2011_10F_plenrep.pdf

[2] Compte tenu de l'étude lancée en parallèle par la Commission européenne (DG Affaires intérieures) sur l'application des dispositions en matière de préservation et de conservation des données et afin d'éviter les doublons, il a été décidé de fusionner les questionnaires du T-CY et de la Commission européenne pour que les Parties puissent répondre aux deux en même temps. La Commission européenne (DG Affaires intérieures) a confié l'élaboration de cette étude au cabinet de consultants Centre for Strategy and Evaluation Services (CSES).

[3] Annexe 2 du rapport de réunion abrégé,
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/tcy2013/tcyreports/TCY_2012_14F_PlenAbrMeetRep.pdf

Réponses reçues :

Etat partie	**Réponses reçues**[4]
1. Albanie	7 juillet 2012
2. Arménie	18 avril 2012
3. Azerbaïdjan	6 avril 2012
4. Bosnie-Herzégovine	18 avril 2012
5. Bulgarie	7 mai 2012
6. Croatie	13 avril 2012
7. Chypre	11 septembre 2012
8. Danemark	[pas de réponse]
9. Estonie	14 mai 2012
10. Finlande	13 avril 2012
11. France	13 avril 2012
12. Géorgie[5]	13 juillet 2012
13. Allemagne	13 avril 2012
14. Hongrie	18 avril 2012
15. Islande	[pas de réponse]
16. Italie	24 septembre 2012
17. Lettonie	12 avril 2012
18. Lituanie	20 avril 2012
19. République de Moldova	9 avril 2012
20. Monténégro	14 mai 2012
21. Pays-Bas	16 avril 2012
22. Norvège	24 avril 2012
23. Portugal	1er mai 2012
24. Roumanie	18 avril 2012
25. Serbie	26 avril 2012
26. Slovaquie	5 novembre 2012
27. Slovénie	13 avril 2012
28. Espagne	18 mai 2012
29. Suisse	18 septembre 2012
30. « L'ex-République yougoslave de Macédoine »	3 mai 2012
31. Ukraine	16 avril 2012
32. Royaume-Uni	25 mai 2012
33. Etats-Unis d'Amérique	14 avril 2012
Total	**31**

[4] Certaines Parties ont fourni ultérieurement des informations supplémentaires.

[5] L'Australie a adhéré à la Convention de Budapest en novembre 2012. D'autres pays l'ont ratifiée après le lancement de l'évaluation : l'Autriche (juin 2012), la Belgique (août 2012), la Géorgie (juin 2012), le Japon (juillet 2012) et Malte (avril 2012). La Géorgie a néanmoins accepté de répondre au questionnaire.

2 Mise en œuvre des articles 16 et 29 sur la préservation rapide

2.1 L'article 16 – Préservation rapide (niveau national)

L'article 16 est une mesure provisoire qui permet aux autorités d'ordonner la préservation immédiate de données déjà stockées dans un système informatique. Il peut s'agir de données de trafic, mais aussi de contenu, et elles peuvent être détenues par toute personne physique ou morale, sans restriction aux prestataires de services internet. Les données « rapidement préservées » sont des données informatiques précises qui peuvent jouer un rôle dans une enquête pénale précise. Bien que des perquisitions et saisies (article 19) ou une injonction de produire (article 18) puissent aussi permettre de préserver l'intégrité de données éphémères nécessaires à une enquête pénale, ces mesures demandent souvent plus de temps, de justifications et d'autorisations que la préservation rapide, qui est une mesure provisoire, et sont plus facilement détectables par le suspect. Le recours à l'article 16 laisse le temps nécessaire pour obtenir l'autorisation d'appliquer les mesures prévues aux articles 18 et 19. Cet outil est particulièrement important dans le cadre d'une coopération internationale : les mesures provisoires prévues aux articles 29 et 30 laissent le temps d'organiser l'entraide, notamment concernant les demandes de données informatiques stockées dans un autre pays (article 31).

L'article 16 n'oblige pas à conserver les données. Son champ d'application est plus étroit, puisqu'il concerne des données précises nécessaires à une enquête précise et toujours stockées dans un système informatique (qui risquent de ne plus être disponibles au moment de la demande d'entraide). Mais il est également plus large, puisqu'il couvre non seulement les données d'inscription et de trafic (comme prévu dans les obligations de conservation des données), mais aussi les données de contenu, et non seulement les prestataires de services, mais aussi toute personne physique ou morale susceptible de détenir des données informatiques nécessaires à l'enquête.

Article 16 – Préservation rapide de données informatiques stockées

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

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

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

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

2.2 Application de l'article 16 : aperçu

Pour évaluer l'application de l'article 16 par les Parties, le T-CY applique les critères suivants :

- La loi autorise-t-elle les autorités répressives
  - à ordonner ou imposer à toute personne morale ou physique détenant des données
  - de préserver rapidement des données électroniques
  - en lien avec toute infraction pénale ?

- Ce pouvoir a-t-il déjà été appliqué ?

2.2.1 Fondement juridique[6]

La moitié des Parties environ disposent d'une réglementation autorisant spécifiquement la préservation rapide de données informatiques stockées. Les autres s'appuient sur d'autres pouvoirs. La plupart des Parties ont aussi défini des obligations de conservation des données.

Les pays suivants ont adopté des dispositions spécifiques pour transposer l'article 16 en droit interne :

- Albanie : article 299/a du Code de procédure pénale (CPP)
- Bulgarie : article 159 CPP
- Finlande : loi sur les mesures coercitives, titre 4, articles 4b et c
- France : article 60-2 CPP
- Hongrie : article 158/A CPP
- Italie : plusieurs dispositions de la loi n° 48 de 2008
- Lettonie : article 191 CPP
- Moldova : article 7 de la loi de prévention et de répression de la cybercriminalité (n° 20-XVI du 3 février 2009)
- Pays-Bas : article 126ni du Code néerlandais de procédure pénale
- Norvège : article 215a de la loi de procédure pénale
- Portugal : article 12 de la loi sur la cybercriminalité (loi n° 109/2009)
- Roumanie : article 54 de la loi 161/2003
- Slovaquie : article 90 du Code de procédure pénale
- Etats-Unis : Code pénal fédéral, titre 18, article 2703(f).

D'autres Parties disent préserver les preuves électroniques via des perquisitions et saisies, des injonctions de produire et autres pouvoirs similaires. Ces approches sont valables au sens de la Convention de Budapest si les pouvoirs concernés permettent d'obtenir rapidement des preuves électroniques relatives à toute infraction pénale et auprès de toute personne morale ou physique détentrice de données[7]. La Convention de Budapest n'impose pas aux Parties de prévoir une

[6] Voir l'annexe pour des extraits des législations nationales.

[7] Comme l'ont montré les discussions lors de la réunion plénière du T-CY en décembre 2012, toutes les Parties ne jugent pas qu'un Etat respecte les exigences de la Convention de Budapest s'il recourt à des perquisitions, des saisies ou des injonctions de produire sans prévoir spécifiquement une injonction de préserver. La plupart des

disposition spécifique de procédure pénale. Des procédures plus générales peuvent être employées. Comme le précise le Rapport explicatif :

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

Néanmoins, comme le suggère la dernière phrase du paragraphe 160 du Rapport explicatif, même si d'autres pouvoirs peuvent s'appliquer, des pouvoirs de préservation spécifiques peuvent s'avérer plus efficaces.

Dans certains pays, les prestataires de services ou d'autres personnes morales ou physiques semblent disposés à préserver d'eux-mêmes les données dans l'attente d'une injonction formelle de produire. Dans certains cas, des accords supplémentaires ont été passés avec les prestataires de services :

- En Azerbaïdjan, sur décision administrative, les prestataires de services ont désigné des « conservateurs » auxquels le ministère de la Sécurité nationale peut demander « d'ordonner rapidement, de façon informelle, la préservation de données ».
- En Géorgie, un protocole d'accord entre les autorités répressives et les prestataires de services internet a été signé en mai 2010.
- En Lituanie, en vertu d'un accord, les principaux prestataires nationaux donnent aux autorités répressives l'accès aux données de trafic et d'inscription.
- En République de Moldova, le ministère public et la Banque nationale ont signé un accord sur la monnaie électronique et le commerce en ligne.
- En Norvège, le plus grand fournisseur d'accès internet (FAI) national a mis en place une unité chargée de répondre 24 heures sur 24 et 7 jours sur 7 aux demandes de la police, et les grands fournisseurs internationaux donnent directement suite aux demandes sous certaines conditions. Des accords spécifiques ont été conclus avec plusieurs FAI concernant le filtrage d'images pédophiles.

Parties estiment qu'une telle approche est valable si les pouvoirs existants permettent effectivement d'obtenir rapidement des preuves électroniques relatives à toute infraction pénale et auprès de toute personne morale ou physique détentrice de données.

D'autres estiment que a) la Convention de Budapest n'interdit pas de remplacer la préservation par des saisies, perquisitions et autres mesures similaires et que b) ces pouvoirs peuvent être limités, conformément à l'article 15 (conditions et sauvegardes). La présente évaluation repose sur le premier point de vue : en l'absence de dispositions spécifiques de préservation, il est acceptable que les Parties recourent à d'autres mesures pour « imposer d'une autre manière » la préservation de données précises, dont des données de trafic, si ces mesures peuvent s'appliquer rapidement et à tous types de données. Si le recours à ces autres mesures est restreint, il peut être conclu qu'une Partie « ne respecte pas » ou « respecte partiellement » l'article 16, selon l'étendue des restrictions. La plupart des Parties estiment que prévoir spécifiquement une mesure provisoire de préservation des données permettrait de respecter les conditions et sauvegardes de l'article 15 avant d'obtenir des données par perquisition, saisie ou divulgation.

- En Roumanie, de bonnes pratiques ont été développées en matière de coopération entre FAI et autorités répressives.

2.2.2 Tout type de données

La plupart des Parties ont répondu que toutes les données visées à l'article 16 étaient couvertes par leur réglementation (données d'inscription/données de trafic et de contenu). L'Arménie et l'Ukraine semblent faire exception, ne couvrant que les données de trafic. En Allemagne, des dispositions distinctes s'appliquent à la perquisition et saisie des données de trafic et des autres données.

Presque toutes les autres Parties (sauf l'Arménie, l'Allemagne, la Norvège[8] et les Etats-Unis) appliquent aussi l'obligation de conserver les données et utilisent abondamment les données conservées. Cependant, cette obligation se limite aux données de trafic, alors que l'article 16 couvre aussi les données de contenu.

Les Parties qui ne s'appuieraient que sur l'obligation de conserver les données n'appliqueraient donc pas pleinement l'article 16.

2.2.3 Toute infraction pénale

L'article 16 prévoit la préservation des données liées à toutes les infractions pénales, et non uniquement aux infractions graves ou à celles qui visent ou utilisent un système informatique (voir l'article 14.2, sur la portée d'application des mesures procédurales).

Les plupart des Parties peuvent demander la préservation de données en rapport avec toute infraction pénale. Dans certains pays, des mesures supplémentaires sont possibles si l'infraction est grave ou relève du crime organisé.

Comme indiqué, la plupart des Parties ont instauré une obligation de conservation de données en vertu de la directive européenne de 2006 sur le sujet. Cette directive comporte une restriction concernant les objectifs poursuivis (accès à des données de trafic, dans le cadre d'enquêtes sur des infractions graves), restriction que beaucoup de Parties ont reprise mais qui n'est pas prévue à l'article 16. Là encore, les Parties qui ne s'appuieraient que sur l'obligation de conserver les données n'appliqueraient donc pas pleinement l'article 16.

Certains signalent en outre que cette restriction risque d'entraîner une situation dans laquelle les autorités répressives pourraient accéder plus facilement aux données de contenu qu'aux données de trafic.

La plupart des Parties appliquent l'article 16.3 : la personne ou l'entité tenue de préserver les données doit garder cette mesure secrète. En Norvège, la personne dont les données ont été préservées doit en être informée au plus tard au moment où les autorités répressives accèdent à ces données, sauf si un tribunal en décide autrement.

2.2.4 Toute personne morale ou physique détenant des données

La plupart des preuves électroniques recherchées dans le cadre d'une enquête ont de fortes chances d'être détenues par des prestataires de services, et la plupart des Parties ont le pouvoir légal, parfois complété par des accords de coopération, d'accéder à ces données ou d'ordonner aux prestataires de

[8] En Norvège, une loi sur la conservation des données a été adoptée par le Parlement en 2011 mais son entrée en vigueur a été repoussée.

services de les préserver. L'obligation de conservation des données est limitée aux prestataires de services.

En revanche, l'article 16 couvre aussi les autres personnes morales et physiques.

Certaines Parties n'appliquent pas pleinement cette exigence, limitant les mécanismes de préservation aux prestataires de services.

2.2.5 Procédures de préservation rapide

La préservation rapide de données détenues par un prestataire de services, par un opérateur ou par un autre gardien de données est une mesure provisoire qui devrait être ordonnée au plus vite, sans autorisation d'une autorité judiciaire, pour laisser le temps d'organiser la saisie ou la production des données.

Dans les pays dotés de dispositions juridiques spécifiques, cette exigence de rapidité semble remplie. Un procureur (le plus souvent), un enquêteur (dans certains pays) ou tout agent public (aux Etats-Unis) peut ordonner la préservation de données informatiques spécifiées en lien avec toute infraction pénale.

Dans la plupart des pays appliquant d'autres mesures, la procédure passe généralement par une ordonnance judiciaire de perquisition et saisie ou par une injonction de produire. Cette décision judiciaire peut être rendue dans les 24 heures – mais elle peut aussi prendre des semaines. Dans des circonstances exceptionnelles ou sous certaines conditions, les mesures peuvent être prises par un procureur ou même par un policier.

Comme déjà noté, la « préservation rapide » est une mesure provisoire, destinée à figer sans tarder des preuves électroniques par nature éphémères en attendant l'application des procédures formelles nécessaires à la divulgation effective des données.

De ce fait, conformément à l'article 16, les conditions à remplir pour ordonner la préservation de preuves électroniques ou pour obtenir cette préservation au moyen d'une perquisition et saisie ou d'une injonction de produire ne devraient pas être trop strictes ou complexes. Au contraire, elles devraient être applicables dans les plus brefs délais.

L'existence d'une injonction spécifique de préservation à titre de mesure préliminaire est donc préférable. Le délai d'obtention d'une perquisition et saisie ou d'une injonction de produire permet ensuite d'appliquer un contrôle judiciaire ou d'autres garanties.

2.2.6 Application concrète

La plupart des Parties considèrent la préservation rapide comme un outil important. Cependant, au contraire des Etats-Unis, qui prononcent chaque année des milliers d'injonctions de préserver, l'application effective de l'article 16 en Europe semble limitée, en particulier dans le cadre d'enquêtes nationales.

Bien que cet article soit souvent appliqué dans certains pays (comme en Bulgarie ou en Moldova), la plupart des Parties expliquent que leurs autorités pénales préfèrent appliquer directement des perquisitions et saisies ou des injonctions de produire et n'ont le plus souvent pas besoin de préserver les données à titre provisoire. D'après les informations fournies, le cas des demandes internationales est différent. Ici, il est plus difficile d'obtenir des autorités judiciaires nationales une ordonnance de

perquisition et saisie ou de production de données, et des mesures provisoires s'avèrent nécessaires pour préserver les preuves.

2.2.7 Pratiques

2.2.7.1 Norvège : intérêt de la préservation

La préservation rapide est surtout nécessaire dans le cadre de demandes internationales. L'absence de dispositions sur la préservation créerait d'importants problèmes lorsque des preuves électroniques sont disponibles hors de Norvège. Les demandes d'entraide judiciaire prennent du temps, et les données auraient de grandes chances d'être supprimées ou modifiées avant le traitement de la demande. Un exemple : dans une récente affaire d'homicide, la police norvégienne a mis un an à accéder à des données de contenu sur Facebook. Ces données sont arrivées en Norvège pendant le procès et se sont avérées importantes pour l'issue de l'affaire : les deux accusés ont été jugés coupables, verdict confirmé en appel.

En Norvège, le plus grand FAI national a mis en place une unité chargée de répondre 24 heures sur 24 et 7 jours sur 7 aux demandes de la police, et les grands fournisseurs internationaux donnent directement suite aux demandes sous certaines conditions.

La plupart des demandes de préservation de la part de la police ou du parquet norvégien ne s'adressent pas à une police étrangère, mais à un petit nombre de grandes multinationales (Facebook, Google, Microsoft etc.), afin qu'elles gèlent certaines données. Certaines de ces entreprises ont des équipes qui se tiennent en permanence prêtes à répondre aux demandes des autorités répressives.

Si ces entreprises donnent suite aux demandes de gel de données de la part d'une police étrangère, c'est probablement parce qu'elles sont de toute façon couvertes par les dispositions internationales en matière de préservation rapide (si leur pays est Partie à la Convention de Budapest). Cette pratique réduit la charge de travail de la police sans porter atteinte aux droits et aux garanties juridiques des usagers. Pour obtenir des données de contenu, il faut toujours adresser une demande d'entraide au pays où se trouve l'entreprise concernée.

Il y a des raisons de penser que l'absence de dispositions sur la préservation encouragerait des entreprises comme Facebook ou Google à ne plus donner suite aux « demandes de gel » de la part de polices étrangères.

Il arrive aussi que les demandes de préservation s'adressent à des entités norvégiennes. Le parquet gagne du temps en émettant lui-même une injonction de produire plutôt qu'en passant par l'intermédiaire d'un tribunal.
Dans les affaires portant sur des données sensibles, par exemple couvertes par le secret professionnel, il peut être préférable que l'injonction de produire soit émise par le tribunal, afin de garantir la régularité de la procédure. Si les demandes de préservation n'existaient pas, les procureurs émettraient peut-être davantage d'injonctions de produire sans passer par un tribunal.

Une demande de préservation n'est pas nécessaire pour obtenir des données d'inscription de base auprès d'entreprises de téléphonie, de FAI et de divers services internet (Facebook, Microsoft etc.).

2.2.7.2 Etats-Unis : intérêt, atouts et difficultés

La préservation est un outil essentiel et souvent utilisé dans les enquêtes aux Etats-Unis. Elle donne aux enquêteurs et aux procureurs le temps d'appliquer la procédure légale nécessaire pour enjoindre à un prestataire de services de divulguer des données. C'est généralement un premier pas vers

l'obtention de données détenues par des prestataires de services. Une demande de préservation n'est pas une demande de divulgation ; le prestataire doit uniquement assurer la persistance des données stockées. Les données préservées par un prestataire de services ne deviennent consultables par les enquêteurs ou les procureurs que lorsqu'une demande appropriée (assignation, ordonnance d'un tribunal ou mandat de perquisition) a été adressée au prestataire.

Les Etats-Unis n'ont pas de législation sur la conservation des données. En l'absence de demande de préservation pour un compte précis, les prestataires sont libres de conserver les données associées à un compte ou de les supprimer, en fonction de leurs pratiques commerciales. Sans demandes de préservation, les enquêteurs perdraient l'accès à un important volume de données.

Principaux atouts :

- tout représentant des autorités répressives peut délivrer une demande de préservation ;
- la procédure est simple et rapide ;
- la préservation donne jusqu'à 180 jours aux enquêteurs pour accomplir les étapes préalables à une demande de divulgation des données ;
- la divulgation des données doit être autorisée par une procédure juridique distincte.

Principales difficultés :

- les enquêteurs n'obtiennent généralement pas d'informations sur le compte, y compris sur son existence, car la loi interdit aux prestataires de services de divulguer ces données sans procédure judiciaire complémentaire ;
- bien que la plupart des grands prestataires gardent le secret sur les demandes de préservation, les prestataires de services sont autorisés à en informer le titulaire du compte, ce qui peut révéler prématurément l'existence d'une enquête.

2.3 Article 29 – Préservation rapide de données informatiques stockées (niveau international)

L'article 29 reprend les dispositions de l'article 16 en les appliquant aux demandes de préservation internationales. Au niveau national, la disponibilité des données peut être assurée par des injonctions de produire ou par des perquisitions et saisies ; au niveau international, les demandes de préservation sont souvent le seul moyen de figer les preuves électroniques d'une infraction pénale dans l'attente d'une demande d'entraide judiciaire.

L'article 35 demande aux Parties de mettre en place des points de contact 24/7 pour faciliter la transmission et l'application de demandes de préservation internationales.

Article 29 – Préservation rapide de données informatiques stockées

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

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

a l'autorité qui demande la préservation ;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;

c les données informatiques stockées à préserver et la nature de leur lien avec l'infraction ;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

e la nécessité de la mesure de préservation ; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

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

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de préservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

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

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

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

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

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

2.4 Application de l'article 29 : aperçu

2.4.1 Fondement juridique

Certaines Parties ont adopté des règles spécifiques aux demandes de préservation internationales :

- Portugal : articles 22 et 23 de loi sur la cybercriminalité (loi n° 109/2009)

- République de Moldova : article 10 de la loi de prévention et de répression de la cybercriminalité (n° 20-XVI du 3 février 2009)
- Roumanie : articles 63 et 64 de la loi 171/2003.

Les Parties qui n'ont pas de dispositions spécifiques concernant les demandes internationales de préservation, mais prévoient des procédures nationales spécifiques en la matière disent pouvoir appliquer ces procédures, par exemple en vertu des lois sur la coopération internationale en matière pénale ou en s'appuyant sur l'article 29 de la Convention de Budapest.

Comme indiqué, plusieurs Parties utilisent des perquisitions et saisies, des injonctions de produire ou d'autres procédures générales pour obtenir des preuves électroniques en l'absence de dispositions de préservation spécifiques. Ces pays semblent avoir plus de difficulté à donner suite aux demandes de préservation internationales. Souvent, une demande formelle d'entraide judiciaire, suivie d'une ordonnance d'un tribunal, est nécessaire pour autoriser l'application de ces mesures et assurer la disponibilité des données.

Cela pourrait expliquer le très faible nombre de demandes de préservation internationales dans les Parties sans procédure de préservation spécifique.

2.4.2 Rôle du Réseau 24/7

Pour faciliter l'application pratique des articles 29 et 30, l'article 35 de la Convention de Budapest demande aux Parties de mettre en place des points de contact joignables 24 heures sur 24 et 7 jours sur 7.

Toutes les Parties ont mis en place de tels points de contact. Certains d'entre eux semblent effectivement actifs dans l'envoi, la réception et le suivi des demandes de préservation internationales. D'autres sont moins actifs, même s'ils disposent des pouvoirs nécessaires. D'autres points de contact sont dans l'incapacité d'envoyer, de recevoir et de suivre des demandes internationales de préservation, faute de fondement juridique national suffisant ou parce que le recours à l'entraide judiciaire est obligatoire.

Etat partie	Point de contact 24/7	Rôle et compétences dans l'envoi et l'exécution de demandes de préservation
1. Albanie	Division Lutte contre la criminalité informatique, ministère de l'Intérieur	Autorisé à envoyer/recevoir des demandes de préservation. Suivi assuré par le parquet
2. Arménie	Division Criminalité de haute technologie – Département « Lutte contre la criminalité organisée » de la police	En l'absence de procédures nationales, le PC 24/7 ne peut émettre de demandes de préservation
3. Azerbaïdjan	Département Lutte contre la criminalité dans le domaine des TI et de la communication, ministère de la Sécurité nationale	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
4. Bosnie-Herzégovine	Section Coopération policière internationale, Interpol, Sarajevo	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
5. Bulgarie	Section Cybercriminalité, Direction générale de la lutte contre la criminalité organisée, ministère de l'Intérieur	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
6. Croatie	Département Criminalité économique et corruption, direction générale de la police	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
7. Chypre	Bureau de police scientifique et de lutte contre la cybercriminalité, siège de la police chypriote	Autorisé à recevoir des demandes, qu'il transmet au ministère de la Justice pour vérification et suites à donner
8. Danemark	Police nationale danoise	
9. Estonie	Bureau des renseignements criminels	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
10. Finlande	Bureau national d'investigation Autre PC : ministère de la Justice	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
11. France	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) Police judiciaire, ministère de l'Intérieur	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
12. Géorgie	Département de police criminelle Ministère de l'Intérieur	Les pouvoirs du point de contact, instauré récemment, doivent encore être testés dans la pratique.
13. Allemagne	Unité Criminalité de haute technologie, Office fédéral de la police judiciaire (BKA)	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
14. Hongrie	Centre de la police pour la Coopération internationale dans l'application du droit Autre PC : Bureau national d'investigation – Unité Criminalité de haute technologie	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite

15. Islande	Commissaire national de la police islandaise	
16. Italie	Servizio Polizia Postale e delle Comunicazioni Autre PC : Parquet de Rome – Section Cybercriminalité	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
17. Lettonie	Unité Coordination des opérations et transmission d'informations, police nationale lettone	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
18. Lituanie	Unité Cybercriminalité, Bureau lituanien de police criminelle	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite (ordonnance n°5-V-1102 du Commissaire général de la police, 12 décembre 2011) Cependant, aucune demande n'a été envoyée/reçue à ce jour
19. République de Moldova	Section Lutte contre la criminalité liée aux TI, Parquet général et : Unité Criminalité de haute technologie	Autorisés à envoyer/recevoir des demandes de préservation et à leur donner suite
20. Monténégro	Direction de la police du Monténégro	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite (via un procureur ou un tribunal)
21. Pays-Bas	Unité Criminalité de haute technologie (NHTCU), police nationale Parquet national	Autorisés à envoyer/recevoir des demandes de préservation et à leur donner suite
22. Norvège	Division Criminalité de haute technologie (Kripos), Service national des enquêtes pénales (NCIS Norvège)	Autorisés à envoyer/recevoir des demandes de préservation (et des demandes d'entraide judiciaire) et à leur donner suite
23. Portugal	Coordinateur des enquêtes pénales au Portugal, police judiciaire	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
24. Roumanie	Service Cybercriminalité, Direction des enquêtes sur le terrorisme et la criminalité organisée, parquet rattaché à la Haute Cour de cassation et de justice Autre PC : Unité Cybercriminalité, Direction générale de lutte contre le crime organisé et le trafic de stupéfiants Bucarest, Roumanie (police nationale roumaine)	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite. Les compétences du parquet comme PC 24/7 sont définies dans la loi sur la cybercriminalité
25. Serbie	Service Lutte contre la criminalité organisée du ministère de l'Intérieur – Département spécial Criminalité de haute technologie Autre PC : Parquet spécialisé dans la criminalité de haute technologie	Les points de contact peuvent enjoindre un FAI de préserver des données, sur la base du CPP (demandes de données).
26. Slovaquie	Bureau national central d'Interpol,	Autorisé à envoyer/recevoir des demandes

	Bureau de coopération policière internationale	de préservation et à leur donner suite
27. Slovénie	Section Coopération policière internationale, Direction de la police criminelle Autre PC : Unité enquêtes cybernétiques, Direction de la police criminelle	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
28. Espagne	Brigada de Investigación Tecnológica, Comisaria General de Policia Judicial, UDEF Central et : Guardia Civil (GC), Grupo de Delitos Telematicos (GDT) (Groupe Criminalité informatique)	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
29. Suisse	Centre opérationnel Fedpol	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
30. « L'ex-République yougoslave de Macédoine »	Ministère public, Skopje	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
31. Ukraine	Sous-département Cybercriminalité, Division Lutte contre la cybercriminalité et la traite des êtres humains, Département de police criminelle	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite (pouvoirs à réexaminer à la lumière du nouveau Code de procédure pénale, novembre 2012)
32. Royaume-Uni	SOCA Cyber	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite
33. Etats-Unis d'Amérique	Section Délinquance informatique et propriété intellectuelle (CCIPS), ministère de la Justice	Autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite

2.4.3 Procédures et expérience

Habituellement, les demandes de préservation internationales sont transmises aux points de contact 24/7, qui ordonnent au prestataire de services ou à une autre personne morale ou physique de préserver les données. Après réception d'une demande formelle d'entraide judiciaire, le plus souvent par le ministère de la Justice, et émission d'une ordonnance judiciaire, le prestataire de services porte les données à la connaissance des autorités nationales, qui les transmet à la Partie requérante.

Cette procédure – avec des déclinaisons selon les contextes nationaux – est suivie par plusieurs Parties, en particulier lorsque les pouvoirs de préservation sont expressément définis par la loi.

Exemple : la Roumanie

- Une demande internationale de préservation rapide envoyée (par courrier électronique) au point de contact 24/7 roumain décrit un cas d'intrusion suivie d'une altération de données. Une unité de police du pays X enquête sur l'affaire. Il est demandé aux autorités roumaines de préserver les données d'inscription et de trafic liées à plusieurs adresses IP (l'heure et la date sont indiqués). D'après le courrier, l'adresse IP est celle d'un prestataire situé à Bucarest.

- Après inscription au registre de l'unité, le procureur vérifie les adresses IP et le prestataire puis ordonne la préservation.
- Si les informations fournies par le pays requérant sont inexactes ou si le prestataire n'existe plus (même si l'entreprise apparaît toujours sur RIPE, etc.), le procureur demande à l'autre partie de rectifier la demande.
- Le pays requérant est aussi informé qu'une lettre rogatoire est nécessaire pour obtenir les informations qui ont été préservées.
- Un bureau territorial roumain demande au point de contact 24/7 de transmettre une demande de préservation rapide au pays X. Il y décrit les faits, précise de quelle infraction il s'agit et demande la préservation des données d'inscription liées à une adresse de courrier électronique (dont le prestataire se trouve dans le pays X) et les données de connexion pour une période spécifique. Il demande aussi la préservation du contenu de la messagerie.
- La demande est conservée dans le registre de l'unité. Le point de contact 24/7 roumain l'envoie par courrier électronique, avec une lettre d'accompagnement, au point de contact 24/7 étranger.

Les Etats-Unis envoient et reçoivent chaque année de centaines de demandes de préservation. D'autres pays également, comme la France, la Moldova ou la Roumanie, utilisent souvent cette possibilité. Il n'existe pas de statistiques fiables sur le recours aux injonctions de préserver. Dans certains pays, plusieurs services sont habilités à envoyer/recevoir des demandes de préservation et à leur donner suite. Ces demandes ne sont pas toujours désignées par le même terme ou peuvent entrer dans une procédure plus large.

Dans l'ensemble cependant, le T-CY estime que les demandes de préservation internationales sont une possibilité sous-utilisée. Cela semble s'expliquer par :

- le manque de clarté des fondements juridiques et la complexité des procédures, dans certains pays ;
- le rôle assez flou des points de contact 24/7 ;
- les connaissances et l'expérience trop limitées concernant l'usage de la procédure ; d'autres moyens sont alors utilisés.

2.5 Application des articles 16 et 29 (préservation rapide au niveau national et international) : évaluation

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
1. Albanie	Procédures nationales (article 16 de la Convention de Budapest) : L'article 299/a du CPP albanais est spécifiquement consacré à la préservation rapide. Il couvre toutes les données, concernant toutes les infractions. Les demandes de préservation sont délivrées par le procureur. Elles peuvent s'adresser à toute personne morale ou physique détenant des données, et non uniquement à des prestataires de services. L'article 101 de la loi 9918 sur les communications électroniques prévoit en outre la conservation des données. L'utilisation de l'article 299/a et donc l'expérience pratique restent limitées à ce jour. Entre autres problèmes, certains prestataires de services n'ont pas les capacités techniques nécessaires à la préservation des données. Procédures internationales (article 29 de la Convention de Budapest) : L'article 299/a CPP (préservation au niveau national) peut s'appliquer, combiné à l'article 505 CPP, à la loi 10193 de 2009 sur les « relations judiciaires avec des autorités étrangères en matière pénale » et à des traités internationaux. Un point de contact 24/7 a été mis en place au sein de la Division Lutte contre la criminalité informatique du ministère de l'Intérieur. Pour que les données préservées soient recueillies et transmises, une demande formelle d'entraide judiciaire est nécessaire. L'Albanie a commencé à appliquer ces dispositions au second semestre 2012.	Article 16 de la Convention de Budapest : L'Albanie respecte l'article 16 de la Convention de Budapest. Il pourrait être utile de davantage former les autorités répressives et les prestataires de services à l'application pratique de l'article 299/a. Article 29 de la Convention de Budapest : L'Albanie respecte l'article 29, et le mécanisme prévu a commencé à fonctionner. Le cadre juridique et institutionnel est en place. Les autorités pourraient promouvoir sa mise en pratique.
2. Arménie	Procédures nationales (article 16 de la Convention de Budapest) : Aucune disposition juridique spécifique répondant aux exigences de l'article 16 n'est en place. Les preuves électroniques sont considérées comme des preuves matérielles. Les dispositions du CPP en matière de perquisition et saisie (articles 225, 226, 239 et 240) sont	Article 16 de la Convention de Budapest : L'Arménie ne respecte pas l'article 16 de la Convention de Budapest. Des perquisitions et saisies et d'autres pouvoirs peuvent être appliqués pour figer des preuves électroniques,

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	applicables. Le CPP s'applique dans la phase d'enquête ; lors de l'enquête préliminaire, il est possible de s'appuyer sur la loi de 2007 sur les activités opérationnelles de renseignement. Une demande de préservation serait possible sur la base d'une décision de justice, mais aucune n'a été formulée à ce jour. Procédures internationales (article 29 de la Convention de Budapest) : Un point de contact 24/7 a été mis en place au sein de la Division Criminalité de haute technologie – Département « Lutte contre la criminalité organisée » de la police. Il n'est cependant pas habilité à émettre des demandes de préservation. Il pourrait utiliser des ordonnances de perquisition et saisie ou de production, mais cela supposerait une demande d'entraide judiciaire suivie d'une décision de justice. L'Arménie n'a donc pas d'expérience en matière de demandes internationales de préservation.	mais pas de façon rapide. L'Arménie coopère avec le Conseil de l'Europe en vue d'une réforme législative. Cette réforme devraient permettre, entre autres, d'appliquer l'article 16. Article 29 de la Convention de Budapest : L'Arménie ne respecte pas l'article 29. La réforme législative susmentionnée devrait y remédier.
3. Azerbaïdjan	Procédures nationales (article 16 de la Convention de Budapest) : Aucune disposition juridique spécifique n'est disponible. D'autres pouvoirs sont utilisés pour obtenir des données (injonctions de produire en vertu de l'article 10 de la loi sur les activités d'enquête, articles 143.2 (collecte des preuves) et 445 (perquisition, saisie, interception etc.) du Code de procédure pénale). Ces pouvoirs ne peuvent être appliqués que sur ordre d'un tribunal (délivré en une ou deux semaines). Cependant, sur la base du CPP, qui donne aux autorités répressives le droit de recueillir des preuves, un accord a été conclu avec les prestataires de services. En vertu de cet accord, les opérateurs de téléphonie mobile, les fournisseurs d'accès internet et les autres prestataires de services ont nommé des « conservateurs » qui peuvent être enjoints de préserver rapidement des données. Ce mécanisme semble bien fonctionner dans la pratique. Aucune décision judiciaire n'est nécessaire pour appliquer cette mesure provisoire de préservation.	Article 16 de la Convention de Budapest : L'Azerbaïdjan respecte partiellement l'article 16. Les pouvoirs d'enquête généraux, combinés à un accord administratif avec les prestataires, permettent de préserver rapidement des preuves électroniques si nécessaire. Cependant, cette possibilité n'existe pas pour les personnes morales ou physiques non couvertes par l'accord en question. Les autorités gagneraient donc peut-être à adopter des dispositions juridiques spécifiques. Le gouvernement semble avoir l'intention de réviser le Code pénal et le Code de procédure pénale à la lumière des normes internationales en

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Procédures internationales (article 29 de la Convention de Budapest) : Les pouvoirs ci-dessus s'appliquent aussi aux demandes internationales. Ces demandes peuvent reposer sur la loi sur l'entraide judiciaire en matière pénale (29 juin 2001), la Convention de Budapest sur la cybercriminalité, la Convention européenne d'entraide judiciaire en matière pénale et d'autres accords. Un point de contact 24/7 a été mis en place au Département Lutte contre la criminalité dans le domaine des TI et de la communication, ministère de la Sécurité nationale. Le PC 24/7 examine les demandes reçues (réciprocité, intérêt pour la sécurité nationale etc.) puis les envoie au chef de la Direction générale de lutte contre la criminalité organisée transnationale, qui en approuve l'exécution et la transmet à l'Unité Cybercriminalité pour qu'elle contacte le FAI. Pour la collecte et la transmission des données, une demande formelle d'entraide judiciaire est nécessaire. Les demandes envoyées ou reçues sont au nombre de quatre ou cinq par an. Le principal problème est la faible coopération de la part des autres pays.	matière de droits de l'homme et de prééminence du droit. Cela serait l'occasion d'appliquer pleinement les dispositions procédurales de la Convention de Budapest, y compris les conditions et sauvegardes (article 15). Article 29 de la Convention de Budapest : L'Azerbaïdjan respecte partiellement l'article 29 de la Convention de Budapest. Les dispositions existantes permettent de recevoir des demandes d'entraide judiciaire et d'y donner rapidement suite. Néanmoins, il serait judicieux d'adopter des dispositions spécifiques sur la préservation, afin de les étendre à d'autres acteurs que les prestataires de services et de renforcer la sécurité juridique.
4. Bosnie-Herzégovine	Procédures nationales (article 16 de la Convention de Budapest) : Aucune disposition juridique spécifique n'est disponible, ni au niveau de l'Etat ni au niveau des entités. L'article 72a du CPP de l'Etat (ainsi que l'article 86a CPP de la Fédération de B-H, l'article 137 CPP de RS (Journal officiel de RS, n° 53/12) et l'article 72a CPP du district de Brčko) autorisent les injonctions de produire « accélérées » dans les cas urgents : un procureur ou un policier (avec l'accord d'un procureur) adresse une demande à un tribunal, qui délivre une injonction de produire. Dans les cas urgents, le procureur peut ordonner la production de données qui restent sous scellés. Il en informe le juge, qui a 72 jours pour délivrer l'injonction. Après ce délai, les scellés peuvent être levés. Il semble que cette possibilité ne soit pas très souvent utilisée.	Article 16 de la Convention de Budapest : La Bosnie-Herzégovine respecte partiellement l'article 16 de la Convention de Budapest. En l'absence d'une disposition juridique spécifique sur la préservation rapide, des « injonctions de produire accélérées » peuvent permettre aux autorités de figer rapidement des données de trafic détenues par des prestataires de services. Cette possibilité n'englobe pas les données de contenu en la possession d'autres personnes morales ou physiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	En outre, l'article 72a du CPP de l'Etat mentionne des « informations concernant l'usage de services de télécommunication », c'est-à-dire des données de trafic ou du même type mais pas le contenu. La Bosnie-Herzégovine a instauré en 2006 l'obligation de conserver les données pendant douze mois (décision du Conseil des ministres de Bosnie-Herzégovine, 14 novembre 2006 ; Journal officiel de Bosnie-Herzégovine, n° 104/06). Procédures internationales (article 29 de la Convention de Budapest) : Bien qu'aucune disposition spécifique n'ait été adoptée, les articles mentionnés ci-dessus concernant les « injonctions de produire accélérées » peuvent aussi s'appliquer aux demandes internationales de données de trafic. En vertu de ces articles combinés à d'autres accords internationaux ou à la loi sur l'entraide judiciaire en matière pénale, l'article 29 de la Convention de Budapest pourrait s'appliquer en ce qui concerne les données de trafic. Un point de contact 24/7 a été mis en place à la Section Coopération policière internationale, Interpol, Sarajevo. Pour que les données soient recueillies et transmises, une demande formelle d'entraide judiciaire est nécessaire. Sur la base des articles 29 et 30 de la Convention, Interpol (Direction de la coordination des polices) a adressé dix demandes aux autorités compétentes aux Etats-Unis et en Suisse. Les réponses ont été positives.	Il serait souhaitable que la Bosnie-Herzégovine réforme ses procédures et adopte des dispositions spécifiques, conformément à la Convention de Budapest. Article 29 de la Convention de Budapest : La Bosnie-Herzégovine respecte partiellement l'article 29 de la Convention de Budapest. Quelques demandes ont été envoyées et reçues. L'application des dispositions existantes en matière de coopération internationale devrait être encouragée. Dans le même temps, il serait souhaitable que la Bosnie-Herzégovine adopte des dispositions spécifiques, conformes à la Convention de Budapest.
5. Bulgarie	Procédures nationales (article 16 de la Convention de Budapest) : Les demandes de préservation sont possibles en vertu d'une disposition plus large, l'article 159 CPP, qui oblige les personnes physiques et morales à « préserver et transmettre » les données informatiques, y compris les données de trafic et les autres éléments présentant un intérêt pour l'affaire. Les demandes peuvent émaner d'un tribunal ou, avant le procès, d'un procureur ou de la police. Ces demandes, semble-t-il, peuvent être obtenues rapidement et sont très	Article 16 de la Convention de Budapest : La Bulgarie respecte l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : La Bulgarie respecte l'article 29 de la Convention

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	fréquentes (plusieurs par semaines). Elles peuvent porter sur tous les types de données et toutes les infractions et concerner une personne physique ou morale. Les pouvoirs de perquisition et saisie peuvent aussi être appliqués. En outre, la loi bulgare sur les communications électroniques réglemente la conservation des données. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Les pouvoirs applicables à la préservation rapide au niveau national peuvent aussi s'appliquer aux demandes internationales. Un point de contact 24/7 a été mis en place à la Section Cybercriminalité, Direction générale de la lutte contre la criminalité organisée, ministère de l'Intérieur. Une demande au PC 24/7 suffit à déclencher une injonction de préserver dans un délai d'un jour. Le PC reçoit environ une demande tous les deux mois.	de Budapest.
6. Croatie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : En Croatie, plusieurs dispositions rendent possible la préservation rapide de preuves électroniques. Ce sont en particulier les articles 261, 263 et 231 du CPP, sur la « saisie temporaire d'objets ». Le procureur, ou un enquêteur ou policier sous ses ordres, peut exécuter la saisie temporaire ou émettre des injonctions. Toutes les personnes physiques ou morales, toutes les infractions pénales et tous les types de données sont concernés. Peuvent s'appliquer en outre les pouvoirs de perquisition (article 257.2 CPP), le recueil spécial de preuves (art. 332 et 333 CPP) et la clause de confidentialité (art. 333.2 CPP) ; les mesures spéciales ne peuvent être prises que pour certaines infractions graves. La Croatie applique également une obligation de conservation (douze mois). <u>Procédures internationales (article 29 de la Convention de Budapest)</u> :	<u>Article 16 de la Convention de Budapest</u> : La Croatie respecte l'article 16 de la Convention de Budapest, même si elle pourrait envisager l'adoption de dispositions spécifiques. <u>Article 29 de la Convention de Budapest</u> : La Croatie respecte l'article 29 de la Convention de Budapest, même si elle pourrait envisager l'adoption de dispositions spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les pouvoirs de préservation rapide au niveau national peuvent aussi s'appliquer aux demandes internationales, sur la base de textes tels que la Convention de Budapest sur la cybercriminalité, la Convention européenne d'entraide judiciaire en matière pénale, des accords bilatéraux, la loi sur l'entraide judiciaire internationale en matière pénale ou le principe de réciprocité. Un point de contact 24/7 a été mis en place au Département Criminalité économique et corruption, Direction générale de la police. Pour que les données soient recueillies et transmises, une demande formelle d'entraide judiciaire est nécessaire. Souvent toutefois, les demandes de préservation ne sont pas suivies de demandes d'entraide judiciaire.	
7. Chypre	Procédures nationales (article 16 de la Convention de Budapest) : Il n'existe pas à Chypre de disposition spécifique sur la préservation rapide des preuves (électroniques ou autres). Cependant, plusieurs dispositions permettent la préservation de données informatiques stockées détenues ou contrôlées par un suspect ou par une autre personne. Par exemple, l'article 6 de la loi de procédure pénale, chap. 155, autorise la police, dans le cadre d'une enquête sur toute infraction pénale, à ordonner au suspect ou à toute autre personne de produire des données informatiques. Ce pouvoir porte sur toutes les données, sauf celles qui ne peuvent être produites que sur mandat judiciaire (c'est-à-dire les données de communication, en vertu de la législation en vigueur – voir plus loin). Ce pouvoir est largement utilisé par la police. Quiconque refuse, sans raison valable, de donner suite aux ordres de la police en vertu de ce pouvoir est passible d'une peine maximale de trois ans de prison. En outre, la police dispose aussi de pouvoirs de perquisition et saisie souvent utilisés pour préserver des données, et appliqués conformément au principe de proportionnalité (voir les articles 25-29 et 32-34 de la loi de procédure pénale, chap. 155). Concernant les données de trafic, en vertu de la loi 183(I)/2007 (qui transpose la directive 2006/24/CE), tous les prestataires de services de communication électronique accessibles	Article 16 de la Convention de Budapest : Chypre respecte partiellement l'article 16 de la Convention de Budapest. Conformément à cet article, le pays pourrait envisager d'adopter des dispositions juridiques spécifiques. Article 29 de la Convention de Budapest : Chypre respecte partiellement l'article 29 de la Convention de Budapest. Conformément à cet article, le pays pourrait envisager d'adopter des dispositions juridiques spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	au public ou de réseaux de communications publiques doivent conserver pendant six mois toutes les données de trafic et de localisation et les autres données nécessaires à l'identification de l'usager ou de la personne inscrite. Conformément à la directive 2006/24/CE, la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque Etat membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme. Les mêmes principes sont exposés dans le Rapport explicatif de la Convention sur la cybercriminalité. Par conséquent, en raison du caractère sensible de ces données et conformément à notre Constitution (article 17), la loi 183(I)/2007 prévoit que la police ne peut accéder à ces données, aux fins d'une enquête, que sur la base d'un mandat judiciaire et concernant des infractions punies d'au moins cinq ans de prison. Il faut noter qu'à Chypre, toutes les infractions couvertes par la Convention sur la cybercriminalité relèvent de ce cas. Par ailleurs, il serait difficile d'accéder à des données de trafic susceptibles de constituer des preuves d'infractions mineures. L'adoption de dispositions spécifiques sur la préservation permettrait à Chypre de figer des preuves électroniques tout en respectant les normes des droits de l'homme et de la prééminence du droit. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Les pouvoirs en vigueur au niveau national peuvent aussi s'appliquer aux demandes internationales, puisque l'article 3.3 de la loi 22(III)/2004 (portant application de la Convention sur la cybercriminalité) prévoit que la loi 23(I)/2001 (sur la coopération internationale en matière pénale) s'applique aux demandes internationales fondées sur la Convention sur la cybercriminalité. Aux termes de l'article 9.9 de la loi 23(I)/2001, tous les pouvoirs de police prévus par la loi de procédure pénale (chap. 155) peuvent être appliqués à l'exécution de demandes internationales. Concernant les données de trafic, les restrictions susmentionnées s'appliquent.	

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Une demande internationale formelle est nécessaire pour lancer la procédure susmentionnée. Une demande comprenant les informations énoncées à l'article 29.2 de la Convention de Budapest serait suffisante. Lorsqu'il reçoit une demande, le point de contact 24/7 l'envoie au ministère de la Justice pour vérification et transmission aux autorités chypriotes compétentes. Cette approche risque de retarder l'exécution des demandes de préservation internationales. Le rôle du point de contact 24/7 semble plus limité que prévu à l'article 35 de la Convention de Budapest. Des dispositions spécifiques en matière de préservation pourraient permettre de figer plus efficacement des preuves électroniques en réponse à une demande internationale.	
8. Danemark	[Le Danemark n'a pas répondu au questionnaire]	Article 16 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par le Danemark. Article 29 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par le Danemark.
9. Estonie	Procédures nationales (article 16 de la Convention de Budapest) : L'Estonie n'a pas adopté de dispositions spécifiques sur la préservation rapide. Cependant, les pouvoirs généraux prévus à l'article 215 du CPP peuvent être utilisés. Ils prévoient l'obligation de donner suite aux ordres et aux demandes des procureurs et des autorités enquêtrices. Le plus souvent, des mandats de perquisition, de saisie et de production sont directement appliqués, plutôt que des mesures provisoires, dans le respect des principes de nécessité et	Article 16 de la Convention de Budapest : L'Estonie respecte partiellement l'article 16 de la Convention de Budapest. La préservation rapide n'est pas appliquée en pratique. L'Estonie pourrait envisager l'adoption de dispositions spécifiques sur la préservation rapide et encourager leur application pratique.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	de proportionnalité. Les prestataires conservent les données d'inscription et de trafic conformément à la loi sur les communications électroniques (art. 111-113). La divulgation des données de trafic n'est autorisée que pour les infractions pénales graves (sanctionnées d'au moins trois ans de prison). Ainsi, la divulgation de données de trafic est plus strictement encadrée que celle des données de contenu. Des accords de coopération ont été conclus avec les principaux prestataires concernant les demandes de données et leur transmission. Procédures internationales (article 29 de la Convention de Budapest) : Il n'y a pas de disposition juridique spéciale sur la préservation, mais il est possible – dans une certaine mesure – d'utiliser les pouvoirs prévus par la législation nationale pour figer des preuves électroniques. Un point de contact 24/7 a été mis en place. Cependant, les pouvoirs existants ne sont pas utilisés pour les demandes de préservation internationales et le pays n'a pas d'expérience pratique dans ce domaine.	Une nouvelle législation entrera en vigueur le 1er janvier 2013. Conformément aux modifications du Code de procédure pénale, la préservation et la divulgation de données (y compris de données de trafic) seront autorisées pour toutes les infractions pénales. Article 29 de la Convention de Budapest : L'Estonie respecte partiellement l'article 29 de la Convention de Budapest, qui n'est cependant pas appliqué en pratique. L'Estonie pourrait envisager l'adoption de dispositions spécifiques.
10. Finlande	Procédures nationales (article 16 de la Convention de Budapest) : La Finlande a adopté une disposition spécifique sur la préservation rapide, au titre 4, article 4b et 4c de la loi sur les mesures coercitives (450/1987) telle que modifiée en 2007 (titre 8, articles 24 à 26 de la loi révisée, n° 806/2011). En pratique cependant, pour les enquêtes nationales, les données sont obtenues par des mesures de saisie. Cette disposition couvre toutes les données, en lien avec toutes les infractions et toutes les personnes physiques ou morales détenant des données. La Finlande a aussi adopté des dispositions sur la conservation des données. Procédures internationales (article 29 de la Convention de Budapest) :	Article 16 de la Convention de Budapest : La Finlande respecte l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : La Finlande respecte l'article 29 de la Convention de Budapest, bien que la disposition concernée n'ait pas encore été appliquée.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	La mesure susmentionnée peut aussi s'appliquer aux demandes internationales. Les motifs généraux de refus de l'entraide sont énumérés aux articles 12 et 13 de la loi sur l'entraide judiciaire internationale en matière pénale (4/1994) (atteinte à la souveraineté, à la sécurité, aux intérêts essentiels ; demande contraire aux principes des droits de l'homme ou à l'ordre public ; infraction politique ou similaire). La loi 4/1994 est une législation générale sur l'entraide judiciaire, qui s'applique aussi aux relations avec les parties non contractantes. Son article 30 prévoit qu'indépendamment des dispositions de la loi, la Finlande fournit l'aide spécifiquement prévue par les conventions internationales, entre autres.	
11. France	Procédures nationales (article 16 de la Convention de Budapest) : Les articles 56-7 et 60-2 du CPP permettent de recueillir rapidement des preuves électroniques au moyen de mesures de saisie ou de préservation. Ces mesures s'appliquent à toutes les données et à toutes les infractions. L'article 60-2 CPP s'applique aux prestataires de services. Les mesures sont appliquées par la police judiciaire sur réquisition d'un procureur. Des formulaires spécifiques sont utilisés pour les demandes de préservation. La France a également adopté des dispositions sur la conservation des données. Procédures internationales (article 29 de la Convention de Budapest) : Les mesures applicables au niveau national pour figer des preuves électroniques par préservation ou saisie sont aussi utilisées pour les demandes internationales. Le plus souvent, les demandes arrivent par courrier électronique au point de contact 24/7, qui s'assure qu'elles sont complètes (si nécessaire, d'autres informations sont demandées au PC requérant). Un accusé de réception est envoyé. Le PC adresse une demande au prestataire de services au moyen d'un formulaire spécifique. Le PC requérant est informé de la réponse du prestataire et invité à envoyer une lettre rogatoire formelle pour obtenir les données. Le point de contact 24/7, qui ordonne aux prestataires de préserver des données en	Article 16 de la Convention de Budapest : La France respecte l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : La France respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	réponse à une demande étrangère, est l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), Direction centrale de la police judicaire. Une demande d'entraide judiciaire est nécessaire pour que les données soient divulguées. Les demandes envoyées/reçues sont au nombre de trois à cinq par mois. Les demandes de préservation sont émises dans les 24 heures. La procédure est jugée efficace. Difficultés : ▪ les procédures et les modes de présentation des demandes reçues ne sont pas uniformes ▪ souvent, les demandes de préservation ne sont pas suivies de demandes d'entraide judiciaire ▪ les relations avec les organismes responsables de l'entraide judiciaire sont trop distendues pour assurer un suivi au moyen d'une coopération judiciaire.	
12. Géorgie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : Aucune disposition spécifique concernant la préservation rapide n'a été adoptée, mais des mandats de perquisition, de saisie et de production sont appliqués (articles 11, 112, 119, 120 ou 136 CPP), ainsi que des « activités opérationnelles d'enquête ». La principale disposition est l'article 136, sur l'injonction de produire, fréquemment utilisé. La condition pour utiliser une telle injonction ou d'autres pouvoirs est celle de la « cause probable ». Il s'agit du plus faible échelon dans la hiérarchie des preuves prévue par le Code de procédure pénal géorgien. Ce niveau de preuve suffit généralement à l'ouverture d'une enquête pénale. Un protocole d'accord entre les autorités répressives et les prestataires de services a été signé en mai 2010. La coopération public/privé sur la base de ce protocole semble bien fonctionner. Il semble que le critère de « cause probable » soit suffisamment souple pour permettre un usage efficace des injonctions de produire. Conformément au paragraphe 11 de l'article 3 (définitions), « on entend par « cause probable » un ensemble d'informations ou de faits qui, associés à l'ensemble des circonstances d'une affaire pénale donnée, permettent de	<u>Article 16 de la Convention de Budapest</u> : La Géorgie respecte partiellement l'article 16 de la Convention de Budapest. Les mandats de perquisition, de saisie et de production, associés à la coopération avec les prestataires de services sur la base d'un protocole d'accord, semblent permettre de figer rapidement des preuves électroniques. La Géorgie pourrait toutefois envisager l'adoption de dispositions spécifiques sur la préservation rapide. <u>Article 29 de la Convention de Budapest</u> : La Géorgie respecte partiellement l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	conclure raisonnablement qu'une personne a probablement commis une infraction pénale ; ce niveau de preuve autorise l'ouverture des activités d'enquête directement prévues par le présent Code et/ou l'imposition de mesures préventives ». Procédures internationales (article 29 de la Convention de Budapest) : Comme indiqué, en l'absence de dispositions spécifiques, d'autres pouvoirs peuvent être utilisés pour figer rapidement des preuves électroniques au niveau national. Les statuts de l'Unité spéciale Cybercriminalité, nouvellement créée au sein du Département central de police criminelle, lui attribuent les fonctions de point de contact 24/7. L'Unité est autorisée à figer des données dans le cadre d'une coopération internationale, conformément à l'article 29, sans devoir passer par l'entraide judiciaire. Aucune demande n'a été envoyée ou reçue à ce jour.	D'après les informations fournies, une nouvelle loi sur la coopération internationale des autorités répressives, qui reflètera pleinement les exigences de l'article 29, est en préparation.
13. Allemagne	Procédures nationales (article 16 de la Convention de Budapest) : Aucune disposition spécifique n'a été adoptée en matière de préservation rapide. Les dispositions concernant l'extraction des données d'inscription, la sauvegarde et la saisie et la collecte de données de trafic permettent « d'imposer d'une autre manière » la préservation des données, comme prévu par l'article 16 de la Convention de Budapest. Elles se sont avérées opérationnelles dans la pratique. Les demandes d'identification d'une personne inscrite sous une adresse IP dynamique, particulièrement pertinentes en pratique, donnent lieu en Allemagne à ce qu'on appelle une « divulgation des données d'existence » (*Bestandsdatenauskunft*). Non limitée à certaines infractions pénales en particulier, elle ne nécessite pas d'autorisation judiciaire. Les autorités chargées des poursuites peuvent exiger la divulgation des données d'inscription (nom et adresse de la personne inscrite, numéros de téléphone attribués et autres données de connexion), en vertu de la disposition générale applicable aux enquêtes (articles 161.1 première phrase et 163 du CPP combinés à l'article 113.1 de la loi sur les télécommunications). La seule condition est que la collecte des données d'inscription soit nécessaire à la poursuite d'une enquête ouverte concernant une infraction pénale. L'accord du tribunal ou du parquet n'est pas nécessaire.	Article 16 de la Convention de Budapest : L'Allemagne respecte l'article 16 de la Convention de Budapest, car des moyens de figer rapidement des preuves existent et sont utilisés en pratique. Cependant, l'Allemagne pourrait envisager l'adoption de dispositions spécifiques sur la préservation pour les procédures nationales et internationales. Cela pourrait rendre le système moins complexe et plus prévisible. Article 29 de la Convention de Budapest : L'Allemagne respecte l'article 29 de la Convention de Budapest, car des moyens de figer rapidement des preuves existent et sont utilisés en pratique. Cependant, l'Allemagne pourrait envisager l'adoption de dispositions spécifiques sur la

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	La Convention est également mise en œuvre par les dispositions générales en matière de saisie (articles 94 et suiv. CPP) et par celles relatives à la collecte de données de trafic (article 100g CPP), qui autorisent la préservation rapide de données de trafic dans le respect du principe de proportionnalité. En principe, les saisies nécessitent un mandat judiciaire. Il est cependant possible d'obtenir rapidement un tel mandat. Les tribunaux ont mis en place une permanence téléphonique, assurée à tour de rôle par les juges, qui permet d'obtenir un mandat judiciaire dans des délais très brefs. Les bureaux du parquet et de la police sont eux aussi joignables en permanence. S'il s'avère exceptionnellement impossible d'obtenir assez vite un mandat judiciaire, l'ordre peut être donné par un procureur ou (sauf pour les données de trafic) par la police. Si le procureur ou la police estiment que les données risquent d'être supprimées à tout moment, ils n'ont pas à demander de mandat judiciaire, mais peuvent – et même doivent – agir d'office. Si nécessaire, ils peuvent ordonner la saisie des données. La saisie peut s'appliquer en lien avec toutes les infractions pénales et toutes les personnes physiques ou morales. Pour les données de trafic stockées par un prestataire, l'article 100g CPP peut s'appliquer. Conformément au principe de proportionnalité, l'accès à de telles données est soumis à des restrictions. Les autorités répressives peuvent obtenir des données de trafic lorsque l'affaire porte sur une infraction pénale suffisamment grave. Les autorités allemandes considèrent ces restrictions comme autorisées par l'article 15 (conditions et sauvegardes). Cependant, il n'est pas toujours possible de connaître d'emblée le degré de gravité d'une infraction. Les restrictions empêchent donc de préserver les données dans le but d'évaluer la situation. Toutefois, les données de trafic peuvent aussi être obtenues lorsqu'une infraction pénale est commise par le biais de moyens de télécommunication, qu'il s'agisse d'une infraction grave ou mineure. C'est le cas lorsqu'une infraction, une escroquerie par exemple, est commise par le biais de courriers électroniques, d'appels téléphoniques ou de sites internet. Ainsi, le seul cas dans lequel les autorités répressives ne peuvent pas obtenir les données de trafic est celui, très limité, d'infractions mineures non commises par le biais de moyens de télécommunication.	préservation pour les procédures nationales et internationales. Cela pourrait simplifier la coopération internationale.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Comme pour la saisie, un mandat judiciaire est en principe nécessaire, mais la mesure peut être ordonnée par un procureur dans certaines circonstances précises. Une disposition spécifique sur la préservation figure à l'article 16b de la loi sur le commerce des titres. Elle concerne les données de trafic en cas de soupçon de délit d'initié ou de manipulation des cours. En Allemagne, les données de trafic ne sont pas conservées en l'absence de soupçon spécifique (*anlasslos*) : la loi portant mise en œuvre de la directive européenne sur la conservation des données a été déclarée anticonstitutionnelle en 2010. Cependant, les prestataires de services de télécommunication continuent de conserver des données de trafic sur la base des articles 96 et suiv. de la loi sur les télécommunications, nonobstant la décision de la Cour constitutionnelle fédérale. L'obtention de ces données obéit aux procédures déjà décrites. Bien que ce système fonctionne en pratique, il semble assez complexe, notamment du fait de la structure fédérale de l'Allemagne. Les différents niveaux risquent d'entraîner des retards et une certaine imprévisibilité. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : En l'absence de dispositions juridiques spécifiques sur la préservation rapide, les articles de la loi sur l'entraide judiciaire internationale (IRG) en matière de perquisition et saisie peuvent s'appliquer. L'article 74 autorise le ministère de la Justice à déléguer la responsabilité des demandes internationales à d'autres organes au niveau de la Fédération ou des Etats. L'article 67 IRG couvre la perquisition et saisie et peut donc être utilisé pour figer des preuves électroniques. Un mandat judiciaire est requis, mais en cas d'urgence, c'est-à-dire lorsque le délai d'obtention du mandat risque d'entraîner la perte de preuves, la perquisition et saisie peut être ordonnée par un procureur. L'article 67.1 prévoit que la perquisition et saisie peut être effectuée avant réception de la lettre rogatoire officielle.	

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Une demande remplissant les exigences formelles de l'article 29.2 de la Convention de Budapest suffit à obtenir la préservation de données en Allemagne. Pour que les données soient divulguées à des autorités étrangères, une demande d'entraide est nécessaire. Un point de contact 24/7 a été mis en place au sein de l'Unité Criminalité de haute technologie, Office fédéral de la police judiciaire (BKA). En général, le point de contact est autorisé à envoyer/recevoir des demandes de préservation et à leur donner suite. Dans le contexte de procédures internationales (art. 29 de la Convention), il sert de premier interlocuteur pour la présentation d'une demande de préservation aux autorités judiciaires ou policières compétentes et pour lancer les étapes suivantes. Bien que l'Allemagne ait coopéré avec succès avec d'autres Parties dans de nombreuses affaires, le système semble assez complexe et difficile à comprendre pour les autorités étrangères.	
14. Hongrie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : L'article 158/A CPP autorise la préservation rapide de toute donnée informatique. L'ordre de préserver est émis par un tribunal, par un procureur ou par les autorités chargées de l'enquête et reste valable au maximum trois mois. En pratique, cette procédure est jugée complexe et sujette à des plaintes et à un contrôle juridictionnel. Les pouvoirs généraux, permettant d'obtenir des données via des injonctions de produire ou des perquisitions et saisies, sont donc plus souvent utilisés. Par ailleurs, des accords de coopération ont été signés avec des prestataires de services. Une réglementation sur la conservation des données a été adoptée. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Concernant les demandes internationales, la Hongrie doit ouvrir sa propre enquête avant de pouvoir préserver des données. Les accords avec les prestataires sont donc souvent utilisés pour préserver des données.	<u>Article 16 de la Convention de Budapest</u> : La Hongrie respecte l'article 16, mais pourrait envisager des mesures pour faciliter l'application pratique de la disposition en matière de préservation. <u>Article 29 de la Convention de Budapest</u> : La Hongrie respecte partiellement l'article 29. La préservation via l'article 158/A CPP est complexe et conditionnée à l'ouverture d'une enquête au niveau national. A ce jour, la disposition n'a pas été mise en pratique. Il faut donc recourir à d'autres accords et pouvoirs. La Hongrie pourrait envisager l'adoption de dispositions spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Le Centre de la police pour la Coopération internationale dans l'application du droit joue le rôle de point de contact 24/7. L'Unité Criminalité de haute technologie du Bureau national d'investigation joue elle aussi ce rôle.	
15. Islande	[L'Islande n'a pas répondu au questionnaire]	Article 16 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par l'Islande. Article 29 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par l'Islande.
16. Italie	Procédures nationales (article 16 de la Convention de Budapest) : La loi n° 48 du 18 mars 2008 a modifié et complété le Code de procédure pénale pour prévoir des mesures urgentes permettant de figer des preuves électroniques. Les nouvelles dispositions figurent à l'article 244 (inspections autorisant la préservation de données), 247 (perquisitions permettant la préservation de données), 248 (injonctions de produire), 254 (saisie de la correspondance), 254bis (élargissant les injonctions de produire aux prestataires de services), 259 (conservation des biens saisis, y compris les données), 352 (perquisitions, comprenant les moyens techniques de préservation des données), 354 (enquêtes et saisies urgentes, y compris de données et de systèmes informatiques). En cas d'urgence ou de flagrant délit, ces mesures peuvent être prises par la police judiciaire ou immédiatement ordonnées par le procureur. Elles s'appliquent à tous les types de données et à toute personne physique ou morale. Procédures internationales (article 29 de la Convention de Budapest) : [pas d'information reçue]	Article 16 de la Convention de Budapest : L'Italie respecte l'article 16. Article 29 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par l'Italie.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
17. Lettonie	Procédures nationales (article 16 de la Convention de Budapest) : L'article 191 CPP porte spécifiquement sur la préservation rapide. Un enquêteur (par exemple de l'Unité Lutte contre la cybercriminalité et protection des droits de propriété intellectuelle) prépare la décision sur la base de la loi de procédure pénale, chapitre 191. Parallèlement, l'enquêteur se met en contact avec le prestataire de services et visite le lieu où les données doivent être préservées (espace technique de stockage du prestataire). Il contrôle la procédure de préservation et le calcul du total de somme. Cette disposition peut être utilisée pour toutes les enquêtes portant sur des données. Un FAI qui divulguerait des informations sur l'enquête serait passible de poursuites. Procédures internationales (article 29 de la Convention de Budapest) : Pour les demandes internationales, la procédure suivante s'applique : ▪ Le point de contact 24/7 (Bureau de coopération internationale du Département central de police criminelle) reçoit la demande et la transmet à l'Unité Lutte contre la cybercriminalité et protection des droits de propriété intellectuelle. ▪ L'Unité communique avec le demandeur pour préciser ses besoins et les informations à préserver. ▪ Elle prépare une demande fondée sur la loi de procédure pénale et sur la loi portant ratification de la Convention. ▪ Parallèlement, l'Unité se met en contact avec le prestataire de service et visite le lieu où les données doivent être préservées (espace technique de stockage du prestataire). ▪ Elle contrôle la procédure de préservation et le calcul du total de somme. ▪ Une fois les données préservées, l'Unité en avertit le point de contact 24/7, au sein de la police. Le point de contact 24/7 reçoit environ deux demandes par mois. La préservation est généralement effective dans un délai d'un jour.	Article 16 de la Convention de Budapest : La Lettonie respecte l'article 16. Article 29 de la Convention de Budapest : La Lettonie respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les données de trafic peuvent être partagées avec d'autres pays ; pour les données de contenu, une demande d'entraide judiciaire est nécessaire. La coopération des autorités avec les prestataires de services est un point fort. En revanche, l'absence dans le CPP d'une disposition spécifique sur les demandes de préservation internationales est jugée problématique.	
18. Lituanie	Procédures nationales (article 16 de la Convention de Budapest) : Plusieurs dispositions sont appliquées pour préserver ou figer par d'autres moyens des preuves électroniques. Il faut notamment citer l'article 155 CPP (droit d'un procureur à obtenir des informations). Une fois ouverte l'enquête préliminaire, l'article 155 prévoit la procédure suivante : L'enquêteur sollicite auprès du procureur l'autorisation de demander la préservation de données. Si le procureur accepte, il adopte une décision, qui doit être approuvée par le juge d'instruction. Lorsque toutes les conditions prévues par la loi sont remplies, la demande est transmise au directeur (ou à un autre responsable compétent) de l'entreprise offrant l'accès au réseau et/ou des services en ligne et les mesures nécessaires sont prises. Les pouvoirs de perquisition et saisie (article 147 CPP) peuvent aussi s'appliquer. La Lituanie prévoit la conservation des données pour les infractions pénales graves, conformément à la loi du 15 avril 2004 sur les communications électroniques. Il est aussi possible d'obtenir des informations sur la base de la loi de 2000 sur les activités de la police et de l'article 10 de la loi sur les activités opérationnelles. Des accords entre la police et les principaux prestataires autorisent également l'accès aux données. Dans la pratique, la préservation rapide n'est pas utilisée au niveau national, du fait de l'existence des mécanismes évoqués ci-dessus (conservation des données, pouvoirs de saisie, de perquisition, d'inspection etc.). Procédures internationales (article 29 de la Convention de Budapest) : Aux termes de l'article 67.5 CPP, « dans les cas prévus par les accords internationaux	Article 16 de la Convention de Budapest : La Lituanie respecte partiellement la Convention de Budapest. La préservation est possible en principe, mais la procédure semble complexe et n'est pas utilisée en pratique. La Lituanie pourrait envisager l'adoption de dispositions spécifiques sur la préservation rapide pour les procédures nationales et internationales. (Le T-CY a été informé que des amendements étaient en cours). Article 29 de la Convention de Budapest : La Lituanie respecte partiellement l'article 29 de la Convention de Budapest, bien que le mécanisme n'ait pas encore pu être testé. Il conviendrait d'encourager l'application effective des demandes de préservation internationales.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	auxquels la République de Lituanie est partie, les tribunaux et les autorités chargées des poursuites et de l'enquête préliminaire donnent suite aux demandes directement reçues des institutions d'autres pays et envoient directement à ces institutions la réponse à leurs demandes ». Il peut ainsi être donné suite aux demandes internationales de préservation en vertu de l'article 29 de la Convention de Budapest. Conformément à l'ordonnance n° 5-V-1102 du Commissaire général de la police, 12 décembre 2011, le PC 24/7 et les points de contact étrangers peuvent se transmettre directement des demandes de préservation. Le point de contact lituanien est l'Unité Cybercriminalité du Bureau lituanien de police criminelle. La Lituanie a reçu plusieurs demandes de l'étranger, mais sans avoir confirmation que la Partie requérante avait l'intention d'envoyer ensuite une demande d'entraide judiciaire (comme prévu à l'article 29.2.f). Les demandes n'ont donc pas été exécutées.	
19. République de Moldova	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : L'article 7 de la loi de prévention et de répression de la cybercriminalité (n° 20-XVI du 3 février 2009) oblige les prestataires de services à préserver les données informatiques demandées pendant une période pouvant aller jusqu'à 120 jours. Ces demandes peuvent porter sur toute infraction pénale. Elles sont émises par un procureur, au moyen d'un formulaire spécifique. Un mandat judiciaire est ensuite nécessaire pour que les données soient produites. Cette mesure, souvent appliquée, est jugée cruciale pour les enquêtes. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : L'article 10 de la loi n° 20-XVI du 3 février 2009 transpose en droit national l'article 29 de la Convention de Budapest. En vertu de l'article 10, une autorité étrangère peut demander aux autorités moldaves la préservation rapide de données informatiques (de contenu) et de données de trafic.	<u>Article 16 de la Convention de Budapest</u> : La Moldova respecte partiellement l'article 16 de la Convention de Budapest. L'article 7 de la loi sur la cybercriminalité est limité aux prestataires de services. A moins que d'autres pouvoirs existants permettent d'ordonner à toute personne physique ou morale de préserver des données, le champ de l'article 7 devrait être élargi. <u>Article 29 de la Convention de Budapest</u> : La Moldova respecte l'article 29 de la Convention de Budapest puisque, pour les demandes

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Le point de contact 24/7 du parquet général et celui de l'Unité Criminalité de haute technologie sont autorisés à ordonner à toute entité (personne physique ou morale) de préserver des données. Les demandes de préservation doivent être soumises par écrit. Les données sont collectées sur la base d'une résolution du parquet général et d'une ordonnance du juge. Elles sont transmises à la suite d'une demande d'entraide judiciaire ; l'ordre de préserver les données reste donc en vigueur pendant au moins 60 jours. D'après les informations fournies, une vingtaine de demandes sont envoyées/reçues chaque mois.	internationales, la préservation n'est pas limitée aux prestataires de services.
20. Monténégro	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : Le Monténégro n'a pas de disposition spécifique sur la préservation rapide, mais la perquisition et saisie (article 75 CPP) et la saisie temporaire (article 85 CPP, incluant les données électroniques) peuvent s'appliquer. Si une perquisition est nécessaire, le mandat est émis par le tribunal à la demande du procureur de l'Etat ou d'un agent de police ayant reçu l'approbation du procureur. La demande est généralement soumise par écrit, mais peut aussi l'être oralement (cas d'urgence, demandes soumises par téléphone, article 76 CPP). Le mandat est émis par le juge d'instruction (à l'écrit). Si nécessaire, la procédure peut être très rapide. Par exemple, si un policier, ayant recueilli l'accord du procureur par téléphone, appelle le juge d'instruction et lui demande d'émettre le mandat, le juge peut obtempérer de suite. Concernant la saisie temporaire (article 85 CPP), le procureur envoie une proposition écrite et le tribunal émet une décision précisant à qui les objets (données électroniques) doivent être saisis et spécifiant qu'ils doivent être préservés soit en étant soumis au tribunal sous une forme lisible et compréhensible, soit d'une autre manière (par exemple, un prestataire internet peut utiliser ses capacités techniques pour préserver les données et les transmettre sur demande au tribunal). En pratique, la préservation est rarement utilisée.	<u>Article 16 de la Convention de Budapest</u> : Le Monténégro respecte l'article 16 de la Convention de Budapest. Il conviendrait cependant qu'il envisage des dispositions spécifiques et encourage leur mise en œuvre dans la pratique. <u>Article 29 de la Convention de Budapest</u> : Le Monténégro respecte partiellement l'article 29 de la Convention de Budapest, bien que le mécanisme n'ait pas encore pu être testé. Il conviendrait d'encourager l'application effective des demandes de préservation internationales.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Procédures internationales (article 29 de la Convention de Budapest) : Les pouvoirs permettant de figer des preuves électroniques au niveau national (perquisition, saisie, saisie temporaire) peuvent aussi s'appliquer aux demandes de préservation internationales. La différence est que dans ce cas, le point de contact 24/7 au sein de la Direction de la police du Monténégro est une personne chargée de contacter le procureur de l'Etat pour qu'il demande au juge d'ouvrir une enquête ou d'émettre un mandat de perquisition ou une proposition de saisie temporaire. Cette personne de contact s'appuie sur les articles de la Convention de Budapest pour expliquer la nécessité de la demande. La procédure suivie est la même que pour les demandes nationales. A ce jour cependant, aucune demande n'a été envoyée ni reçue.	
21. Pays-Bas	Procédures nationales (article 16 de la Convention de Budapest) : L'article 126ni du Code néerlandais de procédure pénale prévoit une disposition spécifique. La procédure est décrite dans le texte de l'article. La demande est émise par le parquet, à l'oral ou à l'écrit. Lorsqu'elle est transmise oralement, une version écrite signée par un procureur doit être transmise dans les trois jours à la partie requise. La demande écrite indique : a. une description précise des données à préserver ; b. la date et l'heure de la demande ; c. les motifs justifiant la demande ; d. la période de préservation demandée ; e. si la demande couvre aussi des données nécessaires pour retrouver l'identité d'autres prestataires dont les réseaux ou services ont été utilisés pour les communications concernées. Le procureur rédige un rapport sur sa demande. La mesure s'applique aux infractions pénales pouvant justifier un placement en détention préventive.	Article 16 de la Convention de Budapest : Les Pays-Bas respectent l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : Les Pays-Bas respectent l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Procédures internationales (article 29 de la Convention de Budapest) : L'article 126ni CPP, concernant la préservation au niveau national, peut aussi s'appliquer aux demandes internationales. La demande est reçue et exécutée par le procureur, qui doit être convaincu que la demande de préservation est fondée. L'Unité Criminalité de haute technologie, qui dépend du parquet spécialisé dans la cybercriminalité, joue le rôle de point focal (24/7) pour la cybercriminalité. Elle contacte ses homologues pour que les demandes de préservation soient transmises à un autre Etat (via son propre point de contact). Cette disposition est fréquemment utilisée, en particulier au niveau international.	
22. Norvège	Procédures nationales (article 16 de la Convention de Budapest) : L'article 215a de la loi de procédure pénale prévoit une disposition spécifique. Elle peut s'appliquer à tout type de donnée et à toute infraction, dans les limites du principe de proportionnalité. Le procureur en charge de l'affaire signe un document adressé à l'entreprise à laquelle il est demandé de figer les données ; puis le policier en charge de l'enquête contacte l'entreprise, le plus souvent par téléphone, et la demande est envoyée à l'entreprise par fax ou courrier électronique. Habituellement, l'entreprise confirme rapidement par fax ou courrier électronique que les données concernées ont été figées pour la période voulue. Si la police ne reçoit pas de confirmation, elle contacte à nouveau l'entreprise pour s'assurer que la demande de préservation est traitée. La conservation des données n'est pas encore prévue en Norvège, ce qui est considéré comme un problème majeur. En effet, les demandes de préservation ou de production arrivent souvent trop tard, alors que les données ne sont déjà plus disponibles. (Un règlement sur la conservation des données devrait entrer en vigueur). Procédures internationales (article 29 de la Convention de Budapest) :	Article 16 de la Convention de Budapest : La Norvège respecte l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : La Norvège respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les dispositions spécifiques concernant la préservation au niveau national peuvent aussi s'appliquer aux demandes internationales. En fait, la préservation est surtout utilisée pour les demandes internationales. Pour les demandes internes à la Norvège, la mesure la plus fréquente est l'injonction de produire. Cette disposition est donc considérée comme importante pour la coopération internationale. Dans la majorité des cas, les demandes de préservation internationales sont traitées par le Service national des enquêtes pénales (Kripos), qui est aussi le point de contact international pour le G8, Interpol et Europol. A la réception d'une demande, le procureur en charge de l'affaire signe un document ordonnant la préservation rapide de données, conformément à l'article 215a de la loi de procédure pénale. L'agent de police compétent contacte l'entreprise qui détient les données pour lui présenter le document, demander confirmation que les données seront préservées et vérifier les coordonnées des personnes responsables de la préservation au sein de l'entreprise. Lorsque les données sont préservées, la police en informe la partie à l'origine de la demande. Cette confirmation est souvent envoyée par courrier électronique. Bien qu'il n'y ait pas de statistiques disponibles, les demandes de préservation sont généralement exécutées le jour même ou le jour ouvrable suivant. Principal atout de la procédure : la préservation peut être ordonnée rapidement. La principale difficulté consiste à obtenir effectivement les données.	
23. Portugal	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : L'article 12 de la loi sur la cybercriminalité (loi n° 109/2009, du 15 septembre 2009) prévoit une disposition spécifique. Les demandes de préservation écrites sont émises par le procureur ou, en cas d'urgence, par la police. Le courrier accompagnant la demande doit décrire la nature des données à préserver, l'origine et la destination de ces données si elles sont connues (en cas de données de trafic) et la période couverte. Cette période est limitée à un maximum de trois mois. Cependant, la demande de préservation peut être renouvelée, par périodes de trois mois au plus, jusqu'à un maximum d'un an.	<u>Article 16 de la Convention de Budapest</u> : Le Portugal respecte l'article 16 de la Convention de Budapest. <u>Article 29 de la Convention de Budapest</u> : Le Portugal respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Une fois la demande émise, le FAI (ou quiconque contrôle les données ou peut y accéder) préserve immédiatement les données concernées et attend, dans le délai fixé, l'arrivée d'un mandat de saisie ou d'une injonction de produire. Si rien ne se passe, la demande de préservation expire et les données sont détruites. La conservation des données est réglementée par une loi séparée (n° 32/2008). <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Les articles 22 et 23 de la loi sur la cybercriminalité (loin° 109/2009) prévoient des dispositions spécifiques applicables aux demandes de préservation internationales. L'article 22 précise la procédure de préservation, l'article 23 les motifs de refus. Le point de contact, au sein de la police judiciaire, peut recevoir les demandes de préservation internationales et leur donner suite. La demande doit répondre aux exigences de la l'article 22 de la loi sur la cybercriminalité et mentionner l'intention de déposer une demande formelle d'entraide pour obtenir une perquisition, la saisie et la divulgation des données. Le pays concerné doit envoyer sa demande à la police judiciaire, qui la transmet à l'autorité judiciaire. Cette autorité adresse une demande de préservation à la personne qui dispose des données ou les contrôle. La police judiciaire peut émettre la demande elle-même en cas d'urgence ou de risque de retard. Elle le signale immédiatement au procureur. Le point de contact 24/7 reçoit souvent des demandes d'aide ou d'information en-dehors des heures de bureau. Elles ne sont pas toujours désignées comme des « demandes de préservation ».	
24. Roumanie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : L'article 54 de la loi n° 161/2003 prévoit une disposition spécifique. Il couvre toutes les données, toutes les infractions pénales et toutes les personnes physiques ou morales. La procédure est décrite à l'article 58 de la loi, auquel la jurisprudence a donné une large interprétation. Si au moins un élément matériel de l'infraction est commis au moyen d'un	<u>Article 16 de la Convention de Budapest</u> : La Roumanie respecte l'article 16 de la Convention de Budapest. <u>Article 29 de la Convention de Budapest</u> :

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	système informatique ou si une preuve de l'infraction est stockée ou a été transmise via un système informatique, les dispositions relatives à la préservation, à la perquisition informatique et à l'interception des communications électroniques s'appliquent. Dès lors que les données risquent d'être perdues, le procureur (agissant d'office ou à la demande de la police judiciaire) adresse une demande de préservation rapide au prestataire ou à la personne qui détient les données. Le juge peut ordonner la préservation de données au cours d'un procès, soit d'office, soit à la demande des participants (procureur, partie lésée ou autre). Le destinataire de la demande est tenu de prendre les mesures nécessaires pour préserver les données/données de trafic, les garder secrètes et assurer techniquement l'intégrité des données concernées. Au plus tard au moment de l'expiration de la demande (90 jours prolongeables de 30 jours), le procureur doit ordonner que les données lui soient remises (« autorisation »). Le prestataire est alors tenu de mettre le matériel contenant les informations préservées à la disposition du procureur pour que des copies puissent être réalisées. Si le prestataire ou le destinataire de l'autorisation ne donne pas suite, le procureur lui adresse un ordre de remise du matériel, dont l'exécution est assurée par lui-même ou par la police judiciaire. Les demandes de préservation sont considérés comme importantes mais ne sont pas très souvent utilisées au niveau national, où la plupart des demandes portent sur des informations liées à des adresses IP. Des accords de coopération informels entre autorités répressives et prestataires de services facilitent la coopération. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Les articles 63 et 64 de la loi n° 171/2003 comportent des dispositions spécifiques sur les demandes de préservation internationales. Ces demandes sont le plus souvent reçues par courrier électronique. Elles sont enregistrées et traitées immédiatement ou le jour ouvrable suivant, le plus souvent par le procureur spécialisé dans la lutte contre la cybercriminalité.	La Roumanie respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Dans tous les cas, le procureur vérifie brièvement les informations reçues (prestataire correctement identifié, heure et date dûment indiquées etc.) avant d'émettre sa demande de préservation. Si les informations s'avèrent inexactes, le procureur demande à ce qu'elles soient rectifiées. Lorsque la demande est envoyée au prestataire, l'autorité étrangère en est informée. Elle est également avertie qu'une lettre rogatoire est nécessaire pour pouvoir récupérer les données. La demande reste généralement valable 90 jours. Si ce délai expire sans que la lettre rogatoire ne soit arrivée, le procureur en informe l'autorité étrangère. A la réception de la lettre rogatoire, le procureur procède comme pour les demandes nationales : il émet une autorisation de présenter les informations préservées et le prestataire est tenu de mettre le matériel à sa disposition pour que des copies puissent être réalisées. Enfin, les informations sont envoyées à l'autorité étrangère par les voies habituelles de coopération internationale. Note : en cas de demande de préservation de données informatiques détenues par une personne physique, l'autorité étrangère est avertie des risques que comporte une telle demande. Le nom de la personne, le lieu où elle se trouve et d'autres informations pertinentes lui sont communiqués. L'avertissement est envoyé lorsque les autorités répressives roumaines estiment qu'une enquête menée par un autre pays pourrait être compromise (cas de petits prestataires de services). Une injonction de produire peut être envoyée au prestataire de services si la demande étrangère montre clairement que seules les données d'inscription sont nécessaires. Au cours des dernières années, la Roumanie a reçu entre dix et quinze demandes de préservation internationales par an. Le principal problème est que toutes ne sont pas suivies d'une demande d'entraide judiciaire ou d'une note signalant que les informations préservées ne sont plus nécessaires. La procédure de demande d'entraide est en effet jugée trop complexe.	
25. Serbie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : La Serbie n'a pas de disposition spécifique sur la préservation rapide mais les articles 85.1,	<u>Article 16 de la Convention de Budapest</u> : La Serbie respecte l'article 16 de la Convention de

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	146 et 255.2 du CPP peuvent être utilisés. Lorsque nécessaire, un policier, un procureur ou un tribunal, selon la phase de la procédure pénale, demande ou ordonne à l'entité de préserver des données stockées spécifiques jusqu'à l'émission d'un mandat de perquisition et saisie. La préservation est utilisée lorsqu'un mandat de perquisition et saisie ou une injonction de produire n'est pas disponible dans l'immédiat. Elle ne s'applique pas qu'à des FAI, mais aussi à des banques, des compagnies d'assurance ou d'autres entités privées détenant des bases de données. La préservation est possible pour tout type d'infraction et de données. Des mesures supplémentaires existent en cas d'infraction grave. L'obligation de conservation des données offre d'autres moyens de figer des preuves électroniques. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Les pouvoirs et procédures existants au niveau national sont aussi appliqués aux demandes de préservation internationales. Les demandes peuvent être reçues et envoyées par le ministère de l'Intérieur, par le Parquet de la République, par le Parquet spécialisé dans la criminalité de haute technologie ou par les tribunaux. Un point de contact 24/7 a été mis en place au ministère de l'Intérieur, département Cybercriminalité du Service de lutte contre la criminalité organisée. Il existe un autre point de contact au sein du Parquet de la République. Les demandes de préservation internationales ne sont pas très souvent utilisées car elles doivent être suivies de demandes d'entraide judiciaire, régies par une procédure complexe.	Budapest, mais devrait envisager des dispositions spécifiques. (Le T-CY a été informé que des propositions d'amendements étaient actuellement débattues). <u>Article 29 de la Convention de Budapest</u> : La Serbie respecte l'article 29 de la Convention de Budapest. Il conviendrait d'encourager l'application effective des demandes de préservation internationales. L'adoption de dispositions spécifiques sur la préservation rapide devrait être envisagée (voir l'observation sur l'article 16). Note : un nouveau CPP doit entrer en vigueur en 2013.
26. Slovaquie	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : Une disposition spécifique existe depuis l'ajout au Code de procédure pénale de l'article 90 (préservation et divulgation de données informatiques). Elle couvre les personnes physiques et morales et tous les types de données. La demande de préservation peut être	<u>Article 16 de la Convention de Budapest</u> : La Slovaquie respecte l'article 16 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	émise par un procureur, sans mandat judiciaire. La mesure est souvent utilisée. Procédures internationales (article 29 de la Convention de Budapest) : L'article 90 CPP peut aussi être utilisé pour donner suite à une demande de préservation internationale. Une lettre rogatoire est nécessaire pour que les données soient divulguées aux autorités étrangères (article 537 et suiv. du Code de procédure pénale). Le Bureau national central d'Interpol joue le rôle de point de contact 24/7. Il est compétent pour envoyer/recevoir des demandes (une soixantaine de demandes par an).	Article 29 de la Convention de Budapest : La Slovaquie respecte l'article 29 de la Convention de Budapest.
27. Slovénie	Procédures nationales (article 16 de la Convention de Budapest) : La Slovénie n'a pas de disposition spécifique sur la préservation rapide, mais les autorités répressives et le parquet utilisent les articles suivants du CPP pour figer des données : • l'article 148, disposition générale qui demande à la police de protéger (c'est-à-dire de préserver) les traces et les objets (dont les données numériques) qui peuvent constituer des preuves • l'article 149b, qui prévoit l'obtention de données de trafic auprès d'opérateurs de télécommunications via un mandat judiciaire • l'article 150, disposition spécifique sur l'interception légale • l'article 164, disposition générale autorisant la police à saisir des objets (dont des preuves numériques) et à fouiller des personnes et/ou perquisitionner leur domicile • l'article 220, qui autorise la police à saisir des objets (dont des objets numériques), y compris temporairement. En pratique, il existe trois possibilités : • Première possibilité : sur la base de l'article 148 CPP, la police demande à l'usager/au propriétaire des preuves numériques de les préserver. La demande est généralement formulée par téléphone ou par courrier électronique, une lettre officielle étant envoyée par la suite. Cela peut prendre très peu de temps – une heure au plus.	Article 16 de la Convention de Budapest : La Slovénie respecte partiellement l'article 16 de la Convention de Budapest. L'adoption de dispositions spécifiques devrait être envisagée. Article 29 de la Convention de Budapest : La Slovénie respecte partiellement l'article 29 de la Convention de Budapest. L'adoption de dispositions spécifiques sur la préservation devrait être envisagée. Il conviendrait de promouvoir l'application des dispositions actuelles en matière de coopération internationale.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	• Deuxième possibilité : si l'usager/propriétaire des données ne coopère pas, ou sur décision de la police (par exemple parce qu'elle prévoit qu'une divulgation partielle sera nécessaire), la police peut saisir des preuves électroniques (y compris temporairement) en vertu des articles 164 et 220. Là aussi, le délai peut être court, pas plus de trois ou quatre jours. • Troisième possibilité : la police obtient un mandat judiciaire (auprès d'un juge d'instruction) puis procède à la saisie des preuves numériques. Lorsque le mandat judiciaire est émis, l'usager/propriétaire des données doit divulguer les preuves électroniques. Cela peut être fait sous 24 heures (le plus souvent dans un délai d'un jour ouvrable). <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Ces trois possibilités et les articles du CPP susmentionnés permettent aussi de donner suite aux demandes internationales de préservation rapide. Ils peuvent s'appliquer à tout sujet (personne, institution, entreprise ou organisation publique ou privée) et à tout type d'infraction pénale. L'article 515 du CPP réglemente la coopération internationale fondée sur l'article 29 et autorise la police/le procureur/le juge à fournir une aide directe à d'autres autorités répressives, y compris par courrier électronique. Le point de contact 24/7 est la Section Coopération policière internationale, Direction de la police criminelle. L'Unité enquêtes cybernétiques, Direction de la police criminelle constitue un autre point de contact. Les demandes internationales sont reçues par la Section Coopération policière internationale. La procédure est ensuite la même que pour l'article 16. A ce jour, la Slovénie n'a reçu que deux ou trois demandes et n'en a jamais envoyé.	
28. Espagne	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : D'après les réponses reçues, l'Espagne a adopté une réglementation sur la conservation	<u>Article 16 de la Convention de Budapest</u> : L'Espagne ne respecte pas l'article 16 de la

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	des données conforme à la directive de l'UE, couvrant les données de trafic et d'inscription et applicable aux prestataires de services, mais pas de disposition sur la préservation rapide au sens de l'article 16 de la Convention de Budapest. En vertu de la jurisprudence, l'accès aux données de trafic conservées est possible en lien avec toute infraction pénale commise au moyen de réseaux informatiques. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : Il n'existe pas de disposition permettant de donner suite aux demandes de préservation internationales.	Convention de Budapest. La réglementation sur la conservation des données décrite dans les réponses ne répond pas aux exigences de l'article 16. Une révision du Code de procédure pénale espagnol serait actuellement envisagée. Cela offrirait l'occasion d'appliquer pleinement l'article 16. <u>Article 29 de la Convention de Budapest</u> : L'Espagne ne respecte pas l'article 29 de la Convention de Budapest.
29. Suisse	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : La Suisse n'a pas de disposition spécifique sur la préservation rapide. Des saisies et des injonctions de produire (articles 263-266) peuvent être utilisées pour figer rapidement des preuves électroniques. Ces pouvoirs formels sont complétés par un accord informel entre les autorités répressives et les principaux prestataires de services internet en matière de préservation des données. Les demandes de préservation peuvent être émises par l'autorité en charge de l'enquête, c'est-à-dire selon le cas par la police, le procureur ou le juge. Ce mécanisme s'est avéré fonctionner dans la pratique, à condition que le responsable concerné connaisse la procédure. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : En vertu de l'article 18 de la loi sur l'entraide judiciaire, les autorités suisses compétentes peuvent prendre des mesures provisoires (comme la préservation des données) aux fins suivantes :	<u>Article 16 de la Convention de Budapest</u> : La Suisse respecte l'article 16 de la Convention de Budapest. <u>Article 29 de la Convention de Budapest</u> : La Suisse respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	- protéger et préserver des intérêts légaux menacés - figer la situation existante, ou - protéger des preuves risquant d'être perdues. Ces mesures peuvent être prises dès que la demande est formulée et aux conditions suivantes : - la procédure ne semble pas irrecevable ou inappropriée - suffisamment de preuves indiquent la nécessité de prendre des mesures provisoires - l'affaire n'est pas considérée comme mineure et non susceptible de justifier l'ouverture d'une enquête. Enfin, si une demande formelle n'est pas présentée dans les délais fixés, la mesure est annulée et les données ne sont pas transmises aux autorités étrangères requérantes.	
30. « L'ex-République yougoslave de Macédoine »	<u>Procédures nationales (article 16 de la Convention de Budapest)</u> : La saisie temporaire prévue aux articles 203 à 206 du CPP (actuel) peut être utilisée pour figer rapidement des preuves électroniques. Elle peut s'appliquer à tous les types de données, à toutes les infractions pénales et à toutes les personnes physiques ou morales. Un mandat du juge d'instruction est nécessaire. Des mesures supplémentaires existent en cas d'infraction pénale grave (article 142b CPP). Ces articles sont souvent utilisés et également appliqués aux banques et autres institutions financières. L'obligation de conservation des données offre d'autres moyens de figer des preuves électroniques. <u>Procédures internationales (article 29 de la Convention de Budapest)</u> : En l'absence de dispositions spécifiques sur la préservation pour les demandes nationales et internationales, les pouvoirs de saisie temporaire et le chapitre XXX de l'actuel Code de procédure pénale, sur la coopération internationale, peuvent être utilisés. L'article 505 peut	<u>Article 16 de la Convention de Budapest</u> : « L'ex-République yougoslave de Macédoine » respecte l'article 16 de la Convention de Budapest. <u>Article 29 de la Convention de Budapest</u> : « L'ex-République yougoslave de Macédoine » respecte l'article 29 de la Convention de Budapest. Le mécanisme n'a pas encore été testé. Il conviendrait d'encourager l'application effective des demandes de préservation internationales.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	servir de base pour donner suite à une demande en vertu de la Convention de Budapest. Le point de contact 24/7 est le Ministère public, à Skopje. Aucune demande de préservation internationale n'a été envoyée ou reçue à ce jour. Note : un nouveau CPP entrera en vigueur le 26 novembre 2013. Son article 184 pourra servir de base à des demandes de préservation.	
31. Ukraine	Procédures nationales (article 16 de la Convention de Budapest) : Le pays n'a pas adopté de disposition spécifique sur la préservation rapide. Un nouveau CPP est entré en vigueur le 19 novembre 2012. Le « prélèvement d'informations sur des systèmes d'information électroniques » est considéré comme une ingérence dans les communications privées (voir l'article 258). Bien que les articles 262 à 265 puissent autoriser l'accès aux données sur mandat judiciaire, ils ne semblent applicables que pour les infractions pénales graves (voir l'article 246.2). Il reste à voir si l'article 259 (préservation d'informations) pourrait s'appliquer. L'obligation de conservation des données (trois ans) offre d'autres possibilités de figer des preuves électroniques, mais en vertu du nouveau CPP, cela pourrait être limité aux infractions pénales graves. Procédures internationales (article 29 de la Convention de Budapest) : Les pouvoirs ci-dessus s'appliquent aussi aux demandes internationales.	Article 16 de la Convention de Budapest : L'Ukraine ne respecte pas l'article 16 de la Convention de Budapest. Il pourrait être nécessaire d'envisager d'autres modifications du nouveau CPP. Article 29 de la Convention de Budapest : L'Ukraine ne respecte pas l'article 29 de la Convention de Budapest. Il pourrait être nécessaire d'envisager d'autres modifications du nouveau CPP.
32. Royaume-Uni	Procédures nationales (article 16 de la Convention de Budapest) : Bien que le Royaume-Uni n'ait pas disposition spécifique sur la préservation rapide, plusieurs pouvoirs permettent de figer rapidement des preuves électroniques. Ce sont notamment l'article 102 de la loi de 2001 sur l'anti-terrorisme, le crime et la sécurité (ATCS) et un code de pratique volontaire fondé sur cet article. Les autorités répressives peuvent aussi s'appuyer sur les dispositions de la loi de 2000 portant réglementation des	Article 16 de la Convention de Budapest : Le Royaume-Uni respecte l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest :

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	pouvoirs d'enquête (RIPA) et sur l'annexe 1 de la loi de 1984 sur la police et les preuves pénales (PACE). La procédure appliquée dépend de l'affaire, mais c'est généralement un policier qui adresse une demande de préservation au propriétaire des données. La police peut obtenir d'un juge un mandat ordonnant de produire des données ou d'y donner accès, conformément à la loi de 1984 sur la police et les preuves pénales (PACE), ou une injonction de produire en vertu de l'article 1 PACE, et se rendre dans les locaux où la préservation doit être effectuée. Elle peut aussi s'appuyer sur la loi RIPA, en suivant la procédure nécessaire pour obtenir un mandat en vertu de cette loi. Ces procédures peuvent être utilisées pour toutes les enquêtes concernant des infractions pénales commises en ligne. Les prestataires de services se sont également montrés d'une aide très précieuse dans les situations d'urgence. Le partage des données entre polices est régi par les lignes directrices du Royaume-Uni sur l'entraide judiciaire. Les propriétaires de données au Royaume-Uni peuvent choisir de fournir des données sans demande d'entraide judiciaire. Les lignes directrices sont disponibles sur : http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary En Ecosse, les mandats de perquisition ordinaires sont utilisés. Les mandats de perquisition, de saisie, d'accès aux informations ou de production des données peuvent être obtenus rapidement. La préservation rapide est jugée cruciale pour les enquêtes, et très souvent plus adaptée que d'autres mesures. L'obligation de conservation des données offre d'autres moyens de figer des preuves électroniques. L'accès aux données conservées peut être obtenu rapidement. Comme les autres pays de l'Union européenne, le R-U possède une législation sur la conservation des données, énoncée dans la réglementation de 2009 sur la conservation des données (directive CE). Procédures internationales (article 29 de la Convention de Budapest) : Les pouvoirs appliqués pour figer rapidement les preuves électroniques au niveau national, associés aux mécanismes existants d'entraide judiciaire, permettent de répondre aux	Le Royaume-Uni respecte l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	demandes internationales. Conformément aux mécanismes d'entraide judiciaire, lorsqu'une demande internationale est reçue et approuvée, les données peuvent être obtenues par le biais de pouvoirs juridiques et d'accords volontaires. Chaque demande est traitée au cas par cas, en tenant compte notamment de la double incrimination. Le point de contact 24/7, situé au sein de l'Agence de lutte contre le crime organisé (SOCA), est compétent pour recevoir les demandes et leur donner suite. La demande doit être adressée à la SOCA, qui l'enregistre et la transmet aux autorités répressives compétentes. Les preuves sont ensuite recueillies et gérées conformément aux règles d'entraide judiciaire, telles qu'énoncées sur http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary	
33. Etats-Unis d'Amérique	Procédures nationales (article 16 de la Convention de Budapest) : La préservation rapide est prévue au titre 18, article 2703(f) du Code pénal fédéral des Etats-Unis. Elle concerne tous les types de données, en lien avec toutes les infractions pénales. Les demandes de préservation n'ont pas à être émises par un juge ou par un procureur. Tout représentant du pouvoir exécutif, y compris un policier, est autorisé à émettre une telle demande. Le plus souvent, lorsqu'une enquête révèle qu'une personne – prestataire de services par exemple – pourrait détenir des données sur un compte intéressant pour l'enquête, l'enquêteur ou le procureur envoie au prestataire une « lettre de préservation ». Cette lettre précise le compte et les types de données à préserver. Elle peut être envoyée par fax, par courrier électronique ou par courrier. Certains grands prestataires disposent de formulaires de demande en ligne. Sur réception de la demande, le prestataire doit agir pour préserver les données concernées. La préservation, considérée comme un outil essentiel, est souvent utilisée dans les enquêtes aux Etats-Unis. Plusieurs milliers de demandes sont émises chaque année. Les Etats-Unis n'ont pas de législation sur la conservation des données.	Article 16 de la Convention de Budapest : Les Etats-Unis respectent l'article 16 de la Convention de Budapest. Article 29 de la Convention de Budapest : Les Etats-Unis respectent l'article 29 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Procédures internationales (article 29 de la Convention de Budapest) : Le fondement juridique de l'exécution des demandes de préservation internationales est le même que pour les demandes nationales. Les principales entités habilitées à recevoir des demandes de préservation internationales et à leur donner suite sont : ▪ le Bureau des affaires internationales, division des affaires pénales, ministère de la Justice ▪ la Section Délinquance informatique et propriété intellectuelle (CCIPS), division des affaires pénales, ministère de la Justice ▪ les représentants des autorités répressives américaines au sein des ambassades des Etats-Unis. En outre, tout représentant du pouvoir exécutif, y compris un policier, peut émettre une demande de préservation internationale. Lorsque le gouvernement étasunien agit au nom d'un gouvernement étranger, toutes les demandes de transfert de données doivent obéir à la procédure d'entraide judiciaire. La préservation des données n'englobe pas la divulgation des données au gouvernement étasunien. Le CCIPS traite des centaines de demandes par an. La préservation est généralement ordonnée dans les 24 heures suivant la réception de la demande.	

3 Mise en œuvre des articles 17 et 30 - Préservation et divulgation rapides de données relatives au trafic (niveau national/international)

3.1 Les articles 17 et 30

3.1.1 L'article 17

L'article 17 complète l'article 16 en prévoyant des obligations spécifiques concernant la divulgation rapide de données de trafic. Il n'est pas rare que les communications en ligne passent par plusieurs prestataires. En vertu de l'article 17, les prestataires de services doivent divulguer suffisamment de données pour permettre de retracer une communication et donc d'adresser des demandes de préservation à tous les prestataires concernés.

Article 17 – Article 17 – Préservation et divulgation rapides de données relatives au trafic

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

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

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

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

3.1.2 L'article 30

L'article 30 complète l'article 29 et constitue le pendant de l'article 17 au niveau international. En vertu de l'article 30, les Parties qui ont reçu une demande de préservation de données en vertu de l'article 29 doivent divulguer à la Partie requérante suffisamment de données pour permettre l'identification de prestataires de services étrangers ayant participé à une communication, afin que d'autres demandes de préservation puissent être envoyées aux Etats concernés.

Article 30 – Divulgation rapide de données préservées

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

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

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

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

3.2 Application des articles 17 et 29 : aperçu

3.2.1 Compétences nationales, procédures et expérience (article 17)

Les pays suivants ont des dispositions juridiques spécifiques sur la préservation et la divulgation rapides de données de trafic :

- Albanie : article 299/b du Code de procédure pénale
- Finlande : loi sur les mesures coercitives, titre 4, article 4b
- Lettonie : disposition spécifique au sein de l'article 191 CPP
- Moldova : article 7f et g de la loi de prévention et de répression de la cybercriminalité (n° 20-XVI du 3 février 2009)
- Pays-Bas : article 126.2 du Code néerlandais de procédure pénale (novembre ??)
- Norvège : loi sur les communications électroniques, article 2-9, et loi de procédure pénale, article 118, premier paragraphe
- Portugal : article 13 de la loi sur la cybercriminalité (loi n° 109/2009)
- Roumanie : article 54 de la loi 161/2003
- Etats-Unis : Code pénal fédéral, titre 18, article 2703(c)

Les autres Parties disent utiliser d'autres pouvoirs, des injonctions de produire le plus souvent, pour obtenir la divulgation de données permettant d'identifier la trajectoire d'une communication et donc d'envoyer des demandes de préservation supplémentaires.

Il s'agit d'une approche acceptable, à condition que la procédure soit rapide et sans complexité excessive. La plupart des Parties utilisant des injonctions de produire et autres pouvoirs indiquent que des mandats judiciaires sont nécessaires mais peuvent être obtenus assez rapidement.

Par ailleurs, seuls quelques pays utilisent fréquemment cette mesure : la Moldova, la Norvège et les Etats-Unis. Ainsi, même lorsque des dispositions juridiques spécifiques existent, elles sont rarement appliquées. En Roumanie, la divulgation partielle est intégrée à la procédure de préservation.

Comme d'autres Parties, la Roumanie a adopté une disposition spécifique, l'article 54.5 de la loi 161/2003. Elle se distingue cependant de la plupart des autres pays car les prestataires de services, lorsqu'ils reçoivent une demande de préservation, sont automatiquement tenus de divulguer suffisamment d'éléments pour permettre de tracer la communication. Une demande séparée de divulgation de données de trafic n'est donc pas nécessaire.

Le Portugal a retenu une approche similaire (article 13 de la loi 109/2009).

Certaines Parties estiment que les obligations de conservation des données rendent cette mesure superflue. A cet égard, un problème particulier, soulevé par l'Estonie et par le Portugal, pourrait aussi se poser dans d'autres pays : dans les pays ayant transposé la directive de l'UE sur la conservation

des données, y compris sa restriction d'objectifs, il peut s'avérer difficile d'obtenir des données de trafic si la demande ne porte pas sur une infraction grave (telle que définie en droit interne).

3.2.2 Procédures et expérience au niveau international (article 30)

Seules quelques Parties (la Bulgarie, la Moldova et la Norvège) semblent utiliser l'article 30. Principale raison, semble-t-il : dans la plupart des Etats, la divulgation partielle de données de trafic et leur transmission à des autorités étrangères supposent une procédure d'entraide judiciaire et ne sont donc pas suffisamment rapides.

Dans certaines Parties, si les autorités du pays requis obtiennent les données de trafic nécessaires en menant leur propre enquête, elles peuvent les partager avec l'autorité requérante.

Opera, prestataire norvégien de services internet, offre un exemple de cas où des données de trafic peuvent conduire à des pays tiers. Opera offre un moteur de recherche pour terminaux mobiles (téléphones portables, etc.), Opera Mini. Ce moteur interroge les sites internet via les serveurs d'Opera, qui les traitent et les compressent avec de les envoyer au terminal mobile. Ce procédé accélère le chargement en réduisant le volume des données chargées. Autre conséquence, les données de trafic des usagers d'Opera Mini dans le monde entier transitent par les serveurs d'Opera en Norvège et dans d'autres pays. Bien qu'Opera Mini ne soit pas un réseau privé virtuel (RPV) ni un serveur proxy à proprement parler, les internautes qui l'utilisent reçoivent une adresse IP norvégienne et il faut contacter Opera pour identifier (si possible) l'usager final. Le NCIS Norvège reçoit régulièrement des demandes internationales concernant Opera.

3.3 Application des articles 17 et 30 (divulgation partielle au niveau national/international) : évaluation

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
1. Albanie	Procédures nationales (article 17 de la Convention de Budapest) : L'article 299/b CPP comporte une disposition spécifique sur la divulgation partielle. La personne qui reçoit l'ordre de préserver les données doit veiller à ce que toutes les données soient disponibles même si la communication a été transmise via plusieurs prestataires de services. Cette personne doit divulguer au procureur ou à la police judiciaire suffisamment d'informations pour permettre l'identification des autres prestataires et la trajectoire de la communication. La mesure n'a pas encore été testée en pratique. Les données de trafic sont également conservées en vertu de la réglementation sur la conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : La procédure vaut aussi pour les demandes internationales. Elle a récemment été appliquée en pratique.	Article 17 de la Convention de Budapest : L'Albanie respecte l'article 17. Article 30 de la Convention de Budapest : L'Albanie respecte l'article 30.
2. Arménie	Procédures nationales (article 17 de la Convention de Budapest) : Aucune disposition juridique spécifique n'est disponible. Il est possible d'utiliser les dispositions du CPP en matière de perquisition et saisie ou, au stade de l'enquête préliminaire, la loi sur les activités opérationnelles. Cependant, il n'y a pas encore d'expérience pratique dans ce domaine. Demandes internationales (article 30 de la Convention de Budapest) : Pas encore de mise en œuvre.	Articles 17 et 30 de la Convention de Budapest : L'Arménie ne respecte pas les articles 17 et 30. L'Arménie coopère avec le Conseil de l'Europe en vue d'une réforme législative. Les autorités pourraient envisager d'appliquer les articles 17 et 30 à cette occasion (voir l'évaluation de l'article 16).

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
3. Azerbaïdjan	Procédures nationales (article 17 de la Convention de Budapest) : Il n'existe pas de disposition juridique spécifique mais une injonction de produire peut être émise, conformément à l'article 10 de la loi sur les activités d'enquête et aux articles 143.2 et 445 du CPP. Pour la production de données de trafic, un mandat judiciaire est nécessaire ; le délai d'obtention est de deux à sept jours. En outre, les demandes administratives de préservation englobent des demandes de divulgation partielle. Cette procédure peut prendre moins d'un jour ouvrable. Ni la préservation, ni la divulgation partielle ne nécessite de mandat judiciaire. Des données de trafic sont également conservées sur la base d'accords bilatéraux entre le ministère de la Sécurité nationale et des prestataires de services, en vertu de l'article 39 de la loi sur les télécommunications. Demandes internationales (article 30 de la Convention de Budapest) : Les demandes internationales peuvent être traitées sur la base de la loi sur l'entraide judiciaire, de la Convention de Budapest, d'autres accords ou du principe de réciprocité. La demande est reçue par le point de contact 24/7 et examinée. Si elle respecte les intérêts de la sécurité nationale et les obligations découlant des accords internationaux, le chef de la Direction générale de lutte contre la criminalité organisée transnationale la transmet à l'Unité Cybercriminalité 2, chargée de contacter les prestataires de services. Une fois recueillies, les données sont envoyées à l'Etat requérant. Aucune procédure d'entraide judiciaire n'est nécessaire pour que suffisamment de données de trafic soient divulguées, conformément à l'article 30. Cette procédure est appliquée quatre à cinq fois par an.	Article 17 de la Convention de Budapest : L'Azerbaïdjan respecte l'article 17, même si les autorités pourraient envisager l'adoption de mesures juridiques spécifiques. Article 30 de la Convention de Budapest : L'Azerbaïdjan respecte l'article 30.
4. Bosnie-Herzégovine	Procédures nationales (article 17 de la Convention de Budapest) : Aucune disposition juridique spécifique n'est disponible, ni au niveau de l'Etat ni au	Article 17 de la Convention de Budapest : La Bosnie-Herzégovine respecte partiellement

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	niveau des entités. Concernant la préservation rapide (article 16 Convention de Budapest), l'article 72a du CPP de l'Etat peut être appliqué (ainsi que l'article 137 du CPP de RS, l'article 86a du CPP de la Fédération et l'article 72a du CPP du district de Brčko). En vertu de cette disposition, un procureur ou un policier (avec l'accord d'un procureur) adresse une demande à un tribunal, qui délivre une injonction de produire. Les autorités n'ont pas d'expérience pratique en matière de divulgation partielle. <u>Demandes internationales (article 30 de la Convention de Budapest)</u> : Un mandat judiciaire est nécessaire pour faire exécuter les demandes de préservation et de divulgation. Ainsi, la divulgation de données de trafic préservées passe par une procédure d'entraide judiciaire. Cependant, l'article 4 de la loi sur l'entraide judiciaire en matière pénale (Journal officiel de B-H n° 53/09) prévoit : « (3) En cas d'urgence, lorsqu'une telle communication est envisagée par un traité international, les demandes d'entraide judiciaire peuvent être transmises et reçues via Interpol ». « (6) Les demandes d'entraide judiciaire sont aussi recevables lorsqu'elles sont transmises par des moyens de télécommunication électroniques ou autres avec une trace écrite, et si l'autorité judiciaire étrangère est prête, sur demande, à délivrer une preuve écrite du mode de transmission et de la demande originale, à condition que ce mode de transmission soit réglementé par un traité international ». Il est donc possible d'appliquer l'article 30 en urgence, même si cela n'a jamais été fait en pratique.	l'article 17. Il serait souhaitable que la Bosnie-Herzégovine réforme ses procédures et adopte des dispositions spécifiques, conformément à la Convention de Budapest. <u>Article 30 de la Convention de Budapest</u> : La Bosnie-Herzégovine respecte partiellement l'article 30.
5. Bulgarie	<u>Procédures nationales (article 17 de la Convention de Budapest)</u> : Les demandes de préservation et de divulgation partielle sont possibles en vertu d'une disposition plus large, l'article 159 CPP, qui oblige les personnes physiques et morales à « préserver et transmettre » les données informatiques, y compris les données de trafic et les autres éléments présentant un intérêt pour l'affaire.	<u>Article 17 de la Convention de Budapest</u> : La Bulgarie respecte l'article 17, même si les autorités pourraient envisager l'adoption de mesures juridiques spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les données de trafic sont également conservées en vertu de la réglementation sur la conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : Il n'existe pas de disposition spéciale sur la divulgation partielle, à des fins nationales comme internationales. Pour les demandes internationales, la Bulgarie use des dispositions générales pour obtenir la pleine divulgation au niveau national mais ne transmet aux autorités étrangères que les informations requises. Une demande formelle d'entraide judiciaire n'est pas nécessaire. Cette approche est bien utilisée en pratique.	Article 30 de la Convention de Budapest : La Bulgarie respecte l'article 30.
6. Croatie	Procédures nationales (article 17 de la Convention de Budapest) : Bien qu'il n'existe aucune disposition spécifique sur la divulgation partielle, une combinaison de mesures peut s'appliquer, par exemple les articles 261 et 263 CPP. L'article 335.2 CPP oblige les prestataires à fournir une assistance technique aux autorités policières. En outre, l'article 68 de la loi sur les pouvoirs et responsabilités de la police donne aux policiers une grande latitude pour demander aux prestataires de « vérifier l'identité, la durée et la fréquence des contacts entre des adresses de télécommunication spécifiées ». La vérification « peut aussi porter sur la détermination du lieu où se trouvent les personnes établissant le contact […] ». Les mesures permettant d'obtenir la divulgation partielle de données de trafic ne sont pas souvent appliquées mais peuvent présenter un intérêt pour certaines enquêtes. Les données de trafic sont aussi conservées en vertu des règles de conservation des données énoncées dans la loi sur les communications électroniques, qui suit globalement la directive sur la conservation des données. La durée de conservation est de douze mois.	Article 17 de la Convention de Budapest : La Croatie respecte l'article 17, même si les autorités pourraient envisager l'adoption de mesures juridiques spécifiques. Article 30 de la Convention de Budapest : La Croatie respecte l'article 30, même si les autorités pourraient envisager l'adoption de mesures juridiques spécifiques et promouvoir l'application de cette disposition dans la pratique.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Demandes internationales (article 30 de la Convention de Budapest) : Aucune demande n'a encore été présentée en vertu de l'article 30. Il n'y a donc pas de pratique établie en ce domaine. Du point de vue formel, il faut noter que le point de contact 24/7 requis par la Convention a été mis en place au Département Criminalité économique et corruption, Direction générale de la police. Ce point de contact peut donner suite aux demandes formulées en vertu de l'article 30 de la Convention et obtenir les informations voulues (données nécessaires pour identifier le prestataire de services et la trajectoire de la communication) par le biais du Centre technico-opérationnel (organisme public autorisé à surveiller les communications et ayant directement accès aux prestataires de services). En général, la loi sur la coopération en matière pénale autorise le point de contact à fournir les informations demandées en vertu de l'article 30 sans demande formelle d'entraide judiciaire, et donc rapidement (en moins de 24 heures).	
7. Chypre	Procédures nationales (article 17 de la Convention de Budapest) : Comme expliqué concernant l'article 16, tous les prestataires de services sont tenus de conserver six mois toutes les données de trafic et de localisation et les autres données nécessaires à l'identification de l'usager ou de la personne inscrite. L'expérience montre que la procédure d'émission d'un mandat judiciaire à cet effet, fondée sur la loi 183(I)/2007, est assez rapide. La demande est préparée par la police. Après vérification et approbation (le même jour) par le parquet général, une demande *ex parte* est adressée au tribunal (le prestataire de services n'en est pas averti). La décision acceptant ou rejetant l'émission du mandat est généralement rendue le jour même. Les restrictions concernant les crimes graves s'appliquent. Demandes internationales (article 30 de la Convention de Budapest) : La divulgation de données de trafic n'est possible qu'en vertu de la loi 183(I)/2007 ;	Article 17 de la Convention de Budapest : Chypre respecte partiellement l'article 17 de la Convention de Budapest. Les autorités devraient peut-être adopter des dispositions juridiques spécifiques. Article 30 de la Convention de Budapest : Chypre ne respecte pas l'article 30 de la Convention de Budapest. Les autorités devraient peut-être adopter des dispositions juridiques spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	elle est soumise aux conditions et sauvegardes prévues par cette loi. La divulgation rapide de données de trafic permettant d'identifier la trajectoire d'une communication ne semble donc pas possible, ou uniquement dans des circonstances limitées.	
8. Danemark	[Le Danemark n'a pas répondu au questionnaire]	Article 17 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par le Danemark. Article 30 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par le Danemark.
9. Estonie	Procédures nationales (article 17 de la Convention de Budapest) : L'Estonie n'a pas adopté de dispositions spécifiques sur la préservation rapide et la divulgation partielle. Cependant, les pouvoirs généraux prévus à l'article 215 du CPP peuvent être utilisés. Ils prévoient l'obligation de donner suite aux ordres et aux demandes des procureurs et des autorités enquêtrices. Le plus souvent, des mandats de perquisition, de saisie et de production sont directement appliqués, plutôt que des mesures provisoires, dans le respect des principes de nécessité et de proportionnalité. Les prestataires conservent les données d'inscription et de trafic conformément à la loi sur les communications électroniques (art. 111-113). La divulgation des données de trafic n'est autorisée que pour les infractions pénales graves (sanctionnées d'au moins trois ans de prison). Ainsi, la divulgation partielle de données de trafic (par le biais d'une saisie, d'injonctions de produire ou de pouvoirs généraux) n'est pas possible pour toutes les infractions pénales. Demandes internationales (article 30 de la Convention de Budapest) : Pour cette mesure, une demande officielle d'entraide judiciaire est nécessaire et les	Article 17 de la Convention de Budapest : L'Estonie respecte partiellement l'article 17 de la Convention de Budapest. La mesure n'est actuellement possible que pour les infractions pénales graves. Une nouvelle législation, qui doit entrer en vigueur le 1er janvier 2013, permettra d'accéder aux données conservées en lien avec un plus large éventail d'infractions. Conformément aux modifications du Code de procédure pénale, la préservation et la divulgation de données (y compris de données de trafic) seront autorisées en lien avec toutes les infractions pénales. Article 30 de la Convention de Budapest :

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	principes de la coopération judiciaire s'appliquent. La mesure n'a pas été testée en pratique. En cas d'urgence, il est possible, avec l'accord du parquet général, de donner suite à une demande présentée via l'Organisation internationale de police criminelle (Interpol) ou le Système d'information Schengen avant que le ministère de la Justice n'ait reçu la demande d'entraide judiciaire.	L'Estonie respecte partiellement l'article 30 de la Convention de Budapest. La mesure n'a pas encore été appliquée. Les procédures formelles d'entraide judiciaire s'appliquent, ce qui laisse supposer que la divulgation rapide de données à la partie requérante est difficile. Cependant, la divulgation rapide peut s'avérer possible en cas d'urgence.
10. Finlande	Procédures nationales (article 17 de la Convention de Budapest) : La Finlande a adopté une disposition spécifique sur la préservation rapide et la divulgation partielle, au titre 4, article 4b et 4c de la loi sur les mesures coercitives (450/1987) telle que modifiée en 2007 (titre 8, articles 24 à 26 de la loi révisée, n° 806/2011). En pratique cependant, pour les enquêtes nationales, les données sont obtenues par des mesures de saisie. Demandes internationales (article 30 de la Convention de Budapest) : La mesure susmentionnée peut aussi s'appliquer aux demandes internationales. Les motifs généraux de refus de l'entraide sont énumérés aux articles 12 et 13 de la loi sur l'entraide judiciaire internationale en matière pénale (4/1994) (atteinte à la souveraineté, à la sécurité, aux intérêts essentiels ; demande contraire aux principes des droits de l'homme ou à l'ordre public ; infraction politique ou similaire). La loi 4/1994 est une législation générale sur l'entraide judiciaire, qui s'applique aussi aux relations avec les parties non contractantes. Il faut noter qu'elle prévoit (article 30) qu'indépendamment des dispositions de la loi, la Finlande fournit l'aide spécifiquement prévue par les conventions internationales, entre autres.	Article 17 de la Convention de Budapest : La Finlande respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : La Finlande respecte l'article 30 de la Convention de Budapest, bien que la disposition n'ait pas encore été appliquée en pratique.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
11. France	Procédures nationales (article 17 de la Convention de Budapest) : La France n'a pas adopté de disposition spécifique sur la divulgation partielle. La saisie ou d'autres pouvoirs peuvent être utilisés. Les prestataires peuvent se voir adresser des demandes de préservation, mais aussi de divulgation partielle. Les données de trafic sont également conservées en vertu de la réglementation sur la conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : La même approche s'applique aux demandes internationales : le prestataire de services qui donne suite à une demande de préservation indique aux autorités répressives si le serveur concerné est géré depuis une adresse IP correspondant à un pays tiers. Les autorités répressives françaises en informent leurs homologues du pays requérant. La mesure est rarement appliquée.	Article 17 de la Convention de Budapest : La France respecte l'article 17. Bien qu'il n'existe pas de mécanisme spécifique à la divulgation partielle, la saisie et d'autres pouvoirs peuvent être appliqués rapidement. Article 30 de la Convention de Budapest : La France respecte l'article 30.
12. Géorgie	Procédures nationales (article 17 de la Convention de Budapest) : Il n'existe pas de disposition spécifique sur la divulgation partielle mais d'autres pouvoirs sont appliqués, dont notamment l'article 136 CPP (injonctions de produire). Ces dernières sont fréquemment utilisées, comme l'a montré une analyse de dix-sept arrêts rendus en 2011 et 2012 après des demandes de données sur les adresses IP et similaires auprès de prestataires de services. L'analyse montre que les prestataires répondent dans un délai de trois jours. Demandes internationales (article 30 de la Convention de Budapest) : La divulgation partielle est possible en vertu de la procédure nationale (article 136 CPP). La Géorgie semble capable de coopérer avec d'autres pays à travers la nouvelle Unité spéciale Cybercriminalité du Département central de police criminelle, qui joue le rôle d'un point de contact 24/7, y compris au regard de la coopération internationale. Il	Article 17 de la Convention de Budapest : La Géorgie respecte partiellement l'article 17 de la Convention de Budapest. L'adoption de dispositions juridiques spécifiques pourrait être envisagée. Article 30 de la Convention de Budapest : La Géorgie respecte partiellement l'article 30 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	serait donc possible de coopérer en vertu de l'article 30 de la Convention de Budapest, même si cela ne s'est encore jamais produit.	
13. Allemagne	Procédures nationales (article 17 de la Convention de Budapest) : En l'absence de disposition spécifique sur la divulgation partielle, l'approche adoptée pour l'article 16 peut aussi l'être pour l'article 17. Cependant, des restrictions s'appliquent pour les données de trafic liées à des infractions dont la gravité n'est pas confirmée ou qui n'ont pas été commises au moyen d'un système informatique. Demandes internationales (article 30 de la Convention de Budapest) : Au niveau national, les données de trafic peuvent être obtenues via les procédures décrites concernant les articles 16 et 29. Une demande présentée en vertu de l'article 29 et comportant suffisamment d'informations (voir l'article 29.2) est considérée comme une demande d'entraide judiciaire valable. Si une telle demande englobe la divulgation partielle de données de trafic, ces données peuvent être divulguées. Cependant, les restrictions déjà citées concernant les données de trafic s'appliquent. En outre, la loi sur l'entraide judiciaire internationale (art. 61 et 92 IRG) permet de transmettre spontanément des informations à la suite d'une demande d'entraide judiciaire.	Article 17 de la Convention de Budapest : L'Allemagne respecte partiellement l'article 17 de la Convention de Budapest. La divulgation de données de trafic est soumise à quelques restrictions. L'adoption de dispositions juridiques spécifiques pourrait être envisagée. Les observations concernant les articles 16 et 29 de la Convention de Budapest s'appliquent ici aussi. Article 30 de la Convention de Budapest : L'Allemagne respecte partiellement l'article 30 de la Convention de Budapest. Les autorités étrangères peuvent se voir transmettre suffisamment de données de trafic, mais des restrictions s'appliquent. Nous renvoyons aux observations concernant les articles 16 et 29.
14. Hongrie	Procédures nationales (article 17 de la Convention de Budapest) : Il n'existe pas de disposition spécifique sur la divulgation partielle, mais des injonctions de saisie peuvent être émises pour obtenir des données de trafic. Demandes internationales (article 30 de la Convention de Budapest) : Il n'existe pas de disposition spécifique, et les moyens d'obtenir des données de trafic	Article 17 de la Convention de Budapest : La Hongrie respecte partiellement l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : La Hongrie ne respecte pas l'article 30 de la

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	et de les divulguer partiellement à des autorités étrangères n'ont pas été testés en pratique. Apparemment, ils supposent la réception d'une demande formelle d'entraide judiciaire et l'ouverture d'une enquête au niveau national.	Convention de Budapest. La divulgation partielle de données de trafic ne semble possible que s'il y a demande formelle d'entraide judiciaire et ouverture d'une enquête nationale.
15. Islande	[L'Islande n'a pas répondu au questionnaire]	Article 17 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par l'Islande. Article 30 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par l'Islande.
16. Italie	Procédures nationales (article 17 de la Convention de Budapest) : L'article 132, paragraphes 1, 1a et 3 de la loi de protection des données peut s'appliquer aux demandes de production de données de trafic : dans le cadre des activités d'enquête, la police judiciaire demande généralement au procureur d'émettre une ordonnance afin d'acquérir les données de trafic nécessaires pour constater l'infraction et en identifier l'auteur ; après avoir vérifié que les conditions légales sont remplies, le procureur émet une ordonnance en vertu de l'article 256 du CPP. La police judiciaire se charge de notifier l'action au fournisseur d'accès internet (FAI) ou autre prestataire de services de communication électronique concerné. Les données demandées sont envoyées à la police judiciaire, qui les transmet à l'autorité judiciaire requérante. Demandes internationales (article 30 de la Convention de Budapest) : La procédure ci-dessus peut aussi s'appliquer aux demandes internationales.	Article 17 de la Convention de Budapest : L'Italie respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : L'Italie respecte l'article 30 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
17. Lettonie	Procédures nationales (article 17 de la Convention de Budapest) : La Lettonie a adopté un disposition spécifique sur la divulgation partielle, l'article 192 CPP. Les conditions sont une décision d'un juge d'instruction ou l'accord du propriétaire des données. En pratique, cette mesure n'est pas jugée intéressante au niveau national, puisque les prestataires de services stockent leurs données en vertu de la réglementation sur la conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : L'article 192 CPP peut aussi s'appliquer aux demandes internationales. La procédure est proche de celle d'une demande de préservation internationale en vertu de l'article 29 de la Convention de Budapest. Si dans le cadre d'une demande de préservation, il s'avère qu'un prestataire de services situé dans un pays tiers a participé à la transmission d'une communication, l'Unité Lutte contre la cybercriminalité et protection des droits de propriété intellectuelle avertit le point de contact 24/7 de Lettonie, qui le signale aussitôt à la Partie requérante. La Lettonie a déjà reçu et traité des demandes de cette nature. Elle a envoyé des demandes similaires à l'étranger, mais l'autre Partie n'a pas divulgué les données.	Article 17 de la Convention de Budapest : La Lettonie respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : La Lettonie respecte l'article 30 de la Convention de Budapest.
18. Lituanie	Procédures nationales (article 17 de la Convention de Budapest) : La Lituanie n'a pas adopté de disposition spécifique sur la divulgation partielle. Les pouvoirs généraux sur l'obtention ou l'obligation de fournir des informations peuvent s'appliquer (article 155 CPP). En fonction de la situation, la divulgation partielle de données de trafic peut être obtenue en vertu de l'article 65.2 de la loi sur les communications électroniques, de l'article 18.1, alinéa 11 de la loi sur les activités de la police ou des articles 147, 155, 205 ou 207 du CPP. Cependant, ces possibilités n'ont pas encore été utilisées en pratique.	Article 17 de la Convention de Budapest : La Lituanie respecte partiellement l'article 17 de la Convention de Budapest. L'adoption de dispositions spécifiques pourrait être envisagée. (Le T-CY a été informé que des amendements étaient en cours). Article 30 de la Convention de Budapest :

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Comme les données de trafic sont déjà conservées en vertu des obligations de conservation des données, la divulgation partielle n'est pas jugée essentielle pour les enquêtes nationales. Des accords ont été signés avec les grands FAI. Il serait donc possible, si nécessaire, d'obtenir rapidement des données. Demandes internationales (article 30 de la Convention de Budapest) : A ce jour, la Lituanie n'a ni envoyé ni reçu de demandes internationales. Une demande d'entraide judiciaire serait nécessaire pour obtenir une divulgation partielle. Cependant, le point de contact 24/7 de la police lituanienne peut appliquer les dispositions de l'article 18.1, alinéa 11 de la loi sur les activités de la police et les articles 30 et 35 de la Convention de Budapest, en s'appuyant sur l'article 3.4 de la loi de la République de Lituanie portant ratification de la Convention de Budapest (n° IX-1974, 22 janvier 2004, entrée en vigueur le 7 mars 2004 ; Journal officiel n° 36-1178, 2004).	La Lituanie respecte partiellement l'article 30 de la Convention de Budapest.
19. République de Moldova	Procédures nationales (article 17 de la Convention de Budapest) : Au niveau national, la divulgation partielle est prévue par l'article 7.2, qui impose aux prestataires de services de fournir aux autorités les informations nécessaires concernant la chaîne de communication. Demandes internationales (article 30 de la Convention de Budapest) : La disposition ci-dessus s'applique aussi aux demandes internationales.	Article 17 de la Convention de Budapest : La Moldova respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : La Moldova respecte l'article 30 de la Convention de Budapest.
20. Monténégro	Procédures nationales (article 17 de la Convention de Budapest) : Le Monténégro n'a pas de disposition spécifique sur la divulgation partielle, mais la perquisition et saisie (article 75 CPP) et la saisie temporaire (article 85 CPP, incluant	Article 17 de la Convention de Budapest : Le Monténégro respecte partiellement l'article 17 de la Convention de Budapest. Le mécanisme n'a

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	les données électroniques) peuvent s'appliquer, comme pour les demandes de préservation. Un mandat judiciaire est requis. Il doit préciser quelles informations supplémentaires doivent être fournies concernant les autres prestataires de services et la trajectoire de la communication. Cependant, ces possibilités n'ont pas encore été utilisées, et les données de trafic sont aussi conservées en vertu des obligations de conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : A ce jour, le Monténégro n'a ni envoyé ni reçu de demandes internationales.	pas encore été mis en pratique. Des dispositions spécifiques sont recommandées. Article 30 de la Convention de Budapest : Le Monténégro respecte partiellement l'article 30, mais le mécanisme demande à être testé en pratique.
21. Pays-Bas	Procédures nationales (article 17 de la Convention de Budapest) : Les Pays-Bas ont adopté une disposition spécifique, l'article 126ni (paragraphe 2) du Code de procédure pénale. Dans le cas d'une infraction pénale grave pouvant donner lieu à une détention préventive (ce qui englobe presque tous les cas de cybercriminalité), le CPP autorise le procureur à ordonner la préservation de données informatiques particulièrement susceptibles d'être perdues ou modifiées. Si ces données portent sur des communications, le prestataire doit aussi fournir les données nécessaires à l'identification d'autres prestataires dont les réseaux ou services ont aussi été utilisés pour la communication concernée. Demandes internationales (article 30 de la Convention de Budapest) : La mesure peut être appliquée rapidement, à travers la coopération entre polices.	Article 17 de la Convention de Budapest : Les Pays-Bas respectent l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : Les Pays-Bas respectent l'article 17 de la Convention de Budapest.
22. Norvège	Procédures nationales (article 17 de la Convention de Budapest) : La divulgation partielle est obtenue sur la base de la loi sur les communications électroniques (article 2-9) et de la loi de procédure pénale (article 118).	Article 17 de la Convention de Budapest : La Norvège respecte l'article 17 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Elle est importante et fréquemment utilisée par la police norvégienne. Les entreprises de télécom peuvent être amenées à fournir des informations sur leurs clients sur la base de la loi sur les télécommunications, article 2-9, troisième partie. Pour les autres données, la demande de données doit être visée et acceptée par l'Autorité des Postes et des Télécommunications. Le cadre juridique changera quand la directive sur la conservation des données aura été transposée. Les demandes de données autres que les informations sur les clients seront examinées par un tribunal. Les prestataires répondent généralement dans les 24 heures. Demandes internationales (article 30 de la Convention de Budapest) : L'article 30, jugé pertinent, est fréquemment appliqué. Il répond à un réel problème en matière de preuves électroniques et de coopération internationale. L'usage accru des RPV et des serveurs proxy complique la situation, puisqu'il oblige à identifier et à recueillir les données pertinentes dans différents lieux et souvent dans différents pays.	Article 30 de la Convention de Budapest : La Norvège respecte l'article 30 de la Convention de Budapest.
23. Portugal	Procédures nationales (article 17 de la Convention de Budapest) : Le Portugal a adopté une disposition spécifique, l'article 13 de la loi sur la cybercriminalité (loi n° 109/2009). Il suffit d'une lettre d'un procureur ou, en cas d'urgence, d'un policier. Les données de trafic sont aussi conservées en vertu de la loi sur la conservation des données. L'accès suppose un mandat judiciaire et il est limité aux infractions pénales graves. Les FAI sont donc moins coopératifs pour la divulgation de données de trafic. Demandes internationales (article 30 de la Convention de Budapest) : Le Portugal a adopté une disposition spécifique concernant les demandes internationales de divulgation partielle (article 22 de la loi n° 109/2009). En vertu de l'article 22.10, les données de trafic montrant qu'une communication est passée par d'autres prestataires de services sont rapidement communiquées à l'autorité étrangère	Article 17 de la Convention de Budapest : Le Portugal respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : Le Portugal respecte l'article 30 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	requérante.	
24. Roumanie	Procédures nationales (article 17 de la Convention de Budapest) : La Roumanie a adopté une disposition spécifique, l'article 54 de la loi n° 161/2003. En vertu de l'article 54.5, les prestataires des services, lorsqu'ils reçoivent une demande de préservation, sont automatiquement tenus de divulguer suffisamment d'éléments pour permettre d'identifier la trajectoire de la communication. Une demande séparée de divulgation de données de trafic n'est donc pas nécessaire. En pratique, les prestataires de services utilisent la divulgation partielle pour informer le procureur lorsqu'ils ne peuvent donner suite à une demande de préservation, pour différentes raisons (service interrompu, nouveaux accords etc.). Les données de trafic sont également conservées en vertu de la réglementation sur la conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : La Roumanie a adopté une disposition spécifique, l'article 64 de la loi n° 161/2003. Le procureur du Service de lutte contre la cybercriminalité peut immédiatement partager les données de trafic partiellement divulguées avec l'autorité étrangère requérante.	Article 17 de la Convention de Budapest : La Roumanie respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : La Roumanie respecte l'article 30 de la Convention de Budapest.
25. Serbie	Procédures nationales (article 17 de la Convention de Budapest) : La Serbie n'a pas de disposition spécifique sur la divulgation partielle, mais plusieurs pouvoirs peuvent être utilisés : le Code pénal (article 112), la loi sur les poursuites publiques (article 5), le Code de procédure pénale actuel (articles 46, 49, 77, 78, 82, 85, 225, 234, 235, 504e, 504ž et 504lj – un nouveau CPP s'applique à compter de 2013), la loi sur l'organisation et les compétences des pouvoirs publics dans la lutte contre la cybercriminalité (articles 2 à 6), la loi sur les communications électroniques (articles 126 à 130) et le règlement encadrant les activités de communication électronique sous le régime de l'autorisation général (articles 31 et 34).	Article 17 de la Convention de Budapest : La Serbie respecte l'article 17 de la Convention de Budapest, mais devrait envisager des dispositions spécifiques. Article 30 de la Convention de Budapest : La Serbie respecte l'article 30, mais devrait envisager des dispositions spécifiques.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	La mesure peut être intéressante au début de l'enquête préliminaire. Lorsque nécessaire, les autorités répressives, le procureur ou le tribunal (selon le stade de la procédure) émettent une demande ou un mandat conformément à la loi. Les données de trafic sont également conservées en vertu des obligations de conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : Les pouvoirs d'enquête nationaux peuvent aussi s'appliquer dans le cas d'une demande internationale d'entraide judiciaire. C'est cependant rarement le cas, la procédure de demande d'entraide étant jugée trop complexe.	
26. Slovaquie	Procédures nationales (article 17 de la Convention de Budapest) : L'article 90 du CPP couvre la préservation et la divulgation de données informatiques, et donc également la divulgation partielle de données de trafic, conformément à l'article 17 de la Convention de Budapest. Il est cependant difficile de savoir si la divulgation partielle est toujours autorisée depuis les modifications récemment apportées au CPP (loi n° 262/2011). Demandes internationales (article 30 de la Convention de Budapest) : [pas d'information reçue]	Article 17 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par la Slovaquie. Article 30 de la Convention de Budapest : Le T-CY n'a pas pu juger du respect de cette disposition par la Slovaquie.
27. Slovénie	Procédures nationales (article 17 de la Convention de Budapest) : La Slovénie n'a pas de disposition spécifique sur la divulgation partielle, mais les procédures mentionnées pour l'article 16 peuvent aussi s'appliquer à l'article 17. En pratique, ces pouvoirs sont rarement utilisés pour obtenir la divulgation partielle.	Article 17 de la Convention de Budapest : La Slovénie respecte partiellement l'article 17 de la Convention de Budapest, bien que le mécanisme doive encore être testé en pratique. La Slovénie pourrait envisager l'adoption de dispositions

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les données de trafic sont également conservées en vertu des obligations de conservation des données. Demandes internationales (article 30 de la Convention de Budapest) : Les procédures mentionnées concernant l'article 29 peuvent aussi s'appliquer à l'article 30. L'article 515 CPP autorise les policiers, procureurs ou juges à fournir une aide directe à des autorités répressives étrangères, par courrier électronique ou moyen similaire. Cet article du CPP slovène peut être utilisé pour la divulgation partielle de données informatiques à d'autres Parties, conformément à l'article 30 de la Convention de Budapest.	juridiques spécifiques. Article 30 de la Convention de Budapest : La Slovénie respecte partiellement l'article 30, bien que le mécanisme doive encore être testé en pratique. La Slovénie pourrait envisager l'adoption de dispositions juridiques spécifiques.
28. Espagne	Procédures nationales (article 17 de la Convention de Budapest) : D'après les réponses reçues, l'Espagne a adopté une réglementation sur la conservation des données conforme à la directive de l'UE, couvrant les données de trafic et d'inscription et applicable aux prestataires de services. Le pays n'a pas de disposition spécifique sur la divulgation partielle. Demandes internationales (article 30 de la Convention de Budapest) : La divulgation partielle supposerait une demande d'entraide judiciaire et ne serait possible qu'en cas d'infraction pénale grave.	Article 17 de la Convention de Budapest : L'Espagne ne respecte pas l'article 17 de la Convention de Budapest. La divulgation de données de trafic n'est possible qu'en cas d'infraction pénale grave. L'Espagne pourrait envisager l'adoption de dispositions juridiques spécifiques. Article 30 de la Convention de Budapest : L'Espagne ne respecte par l'article 30.
29. Suisse	Procédures nationales (article 17 de la Convention de Budapest) : La Suisse n'a pas disposition spécifique à cet égard. L'article 273 CPP autorise les autorités chargées des poursuites à demander la divulgation de données de trafic, de facturation et d'inscription lorsqu'une infraction (pénale ou autre) est soupçonnée. La demande doit être approuvée par un tribunal. Cette possibilité n'est pas limitée à	Article 17 de la Convention de Budapest : La Suisse respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest :

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	certaines infractions pénales. Elle est d'application générale et peut être employée a posteriori. La loi sur la surveillance de la correspondance s'applique aussi. En vertu de son article 14.4, les fournisseurs d'accès internet sont tenus de fournir à l'autorité compétente toute indication permettant d'identifier l'auteur d'un acte punissable commis au moyen d'internet. Etant donné que cette mesure n'est pas considérée comme une mesure de surveillance au sens strict, la demande peut être formulée directement, indépendamment de la gravité de l'acte. Si les conditions de l'article 273 CPP sont remplies, le ministère public peut exiger que lui soient fournies les données de trafic, de facturation ou d'inscription. Dans les 24 heures à compter du moment où les renseignements sont fournis, le ministère transmet les documents nécessaires pour autorisation par le tribunal des mesures de contrainte. Le tribunal statue dans les cinq jours à compter du moment où la surveillance a été ordonnée ou les renseignements fournis (art. 274 CPP). Demandes internationales (article 30 de la Convention de Budapest) : Informations insuffisantes	Le T-CY n'a pas pu juger du respect de cette disposition par la Suisse.
30. « L'ex-République yougoslave de Macédoine »	Procédures nationales (article 17 de la Convention de Budapest) : Le pays n'a pas de disposition spécifique sur la divulgation partielle. Cependant, les mesures de saisie (article 203 CPP) peuvent être utilisées, ainsi que l'article 142b (moyens spéciaux d'enquête pour les infractions pénales graves, y compris la perquisition et saisie de systèmes informatiques ou de bases de données). Un mandat d'un juge d'instruction est nécessaire. Le mécanisme n'a pas encore été mis en pratique. Le nouveau CPP, qui entrera en vigueur le 26 novembre 2013, ne comprend pas de disposition spécifique, mais l'article 184 (perquisition de systèmes et de données informatiques) peut être utilisé. Demandes internationales (article 30 de la Convention de Budapest) :	Article 17 de la Convention de Budapest : « L'ex-République yougoslave de Macédoine » respecte partiellement l'article 17 de la Convention de Budapest. Le mécanisme n'a pas encore été mis en pratique. Des dispositions spécifiques devraient être envisagées. Article 30 de la Convention de Budapest : « L'ex-République yougoslave de Macédoine » respecte partiellement l'article 30 de la Convention de Budapest.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Les mesures susmentionnées peuvent aussi s'appliquer aux demandes internationales. Note : il reste à vérifier comment les mesures prévues aux articles 17 et 30 peuvent s'appliquer en vertu du nouveau Code de procédure pénale (à compter du 26 novembre 2013).	
31. Ukraine	Procédures nationales (article 17 de la Convention de Budapest) : Le pays n'a pas de disposition spécifique sur la divulgation partielle. Un nouveau CPP est entré en vigueur le 19 novembre 2012. La divulgation partielle y est considérée comme une ingérence dans les communications privées, uniquement possible sur mandat judiciaire et pour les infractions pénales graves. Les infractions informatiques énoncées dans le Code pénal ukrainien (articles 361 à 363.1) ne sont pas considérées comme graves. La divulgation partielle ne serait donc possible que si ces infractions sont associées à une infraction grave. Demandes internationales (article 30 de la Convention de Budapest) : Une demande d'entraide judiciaire est nécessaire pour obtenir la divulgation de données de trafic. Les restrictions ci-dessus s'appliquent.	Article 17 de la Convention de Budapest : L'Ukraine ne respecte par l'article 17. Elle pourrait envisager des amendements à son Code de procédure pénale. Article 30 de la Convention de Budapest : L'Ukraine ne respecte pas l'article 30.
32. Royaume-Uni	Procédures nationales (article 17 de la Convention de Budapest) : Le Royaume-Uni n'a pas de disposition spécifique sur la divulgation partielle. Pour déterminer la trajectoire d'une communication, plusieurs pouvoirs peuvent être utilisés – comme pour la préservation rapide. Ce sont par exemple les réglementations de 2009 sur la conservation des données et le Code de pratique sur l'acquisition et la divulgation de données de communication, fondé sur l'article 71 de la loi de 2000 portant réglementation des pouvoirs d'enquête. L'accès aux données conservées peut être obtenu rapidement à travers diverses	Article 17 de la Convention de Budapest : Le Royaume-Uni respecte l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : Le Royaume-Uni respecte l'article 30 de la Convention de Budapest. Les informations peuvent être fournies via la coopération entre polices.

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	dispositions. Ce sont notamment l'article 102 de la loi de 2001 sur l'anti-terrorisme, le crime et la sécurité (ATCS) et un code de pratique volontaire fondé sur cet article. Les autorités répressives peuvent aussi s'appuyer sur les dispositions de la loi de 2000 portant réglementation des pouvoirs d'enquête (RIPA) et sur l'annexe 1 de la loi de 1984 sur la police et les preuves pénales (PACE). La procédure appliquée dépend de l'affaire, mais c'est généralement un policier qui adresse une demande de préservation au propriétaire des données. La police peut obtenir d'un juge un mandat ordonnant de produire des données ou d'y donner accès, conformément à la loi de 1984 sur la police et les preuves pénales (PACE), ou une injonction de produire en vertu de l'article 1 PACE, et se rendre dans les locaux où la préservation doit être effectuée. Elle peut aussi s'appuyer sur la loi RIPA, en suivant la procédure nécessaire pour obtenir un mandat en vertu de cette loi. Ces procédures peuvent être utilisées pour toutes les enquêtes concernant des infractions pénales commises en ligne. Les prestataires de services se sont également montrés d'une aide très précieuse dans les situations d'urgence. Le partage des données entre polices est régi par les lignes directrices du Royaume-Uni sur l'entraide judiciaire, consultables sur : http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary En Ecosse, les mesures de perquisition ordinaires sont utilisées. Demandes internationales (article 30 de la Convention de Budapest) : Comme pour l'article 17, les pouvoirs appliqués pour figer rapidement les preuves électroniques au niveau national, associés aux mécanismes existants d'entraide judiciaire, permettent de répondre aux demandes internationales. Conformément aux mécanismes d'entraide judiciaire, lorsqu'une demande internationale est reçue et approuvée, les données peuvent être obtenues par le biais de pouvoirs légaux et d'accords volontaires. Chaque demande est traitée au cas par cas, en tenant compte notamment de la double incrimination.	

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Le point de contact 24/7, situé au sein de l'Agence de lutte contre le crime organisé (SOCA), est compétent pour recevoir les demandes et leur donner suite. La demande doit être adressée à la SOCA, qui l'enregistre et la transmet aux autorités répressives compétentes. Les preuves sont ensuite recueillies et gérées conformément aux règles d'entraide judiciaire. Ces procédures peuvent être utilisées pour toutes les enquêtes concernant des infractions pénales commises en ligne. Les prestataires de services se sont également montrés d'une aide très précieuse dans les situations d'urgence. Le partage des données entre polices est régi par les lignes directrices du Royaume-Uni sur l'entraide judiciaire. Les propriétaires de données au Royaume-Uni peuvent aussi choisir de fournir des données sans demande d'entraide judiciaire. Les lignes directrices sont consultables sur : http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary La divulgation partielle est donc possible à travers la coopération entre polices. Le Royaume-Uni peut fournir les données obtenues en vertu de l'article 17 à d'autres pays soit en vertu des accords d'entraide judiciaire, soit via un transfert entre polices, comme énoncé dans les lignes directrices, en fonction des demandes de l'Etat requérant.	
33. Etats-Unis d'Amérique	Procédures nationales (article 17 de la Convention de Budapest) : Les autorités répressives obtiennent la divulgation partielle de données de trafic au moyen d'une assignation, comme prévu au titre 18, article 2703(c) du Code pénal fédéral, ou d'une injonction de produire (article 2703(d)). Lorsque l'enquête révèle qu'un prestataire de services pourrait détenir des données intéressantes, l'enquêteur peut demander au procureur d'émettre une assignation ou une injonction de produire pour que les données de trafic (et d'autres données d'inscription) soient partiellement divulguées. On estime à plusieurs milliers par an le nombre d'assignations et d'injonctions de divulgation partielle de données de trafic et d'inscription émises par les entités fédérales.	Article 17 de la Convention de Budapest : Les Etats-Unis respectent l'article 17 de la Convention de Budapest. Article 30 de la Convention de Budapest : Les Etats-Unis respectent partiellement l'article 30 de la Convention de Budapest. Pour les prestataires amont situés aux Etats-Unis, la divulgation partielle et la transmission de données de trafic aux autorités étrangères requérantes

Etat partie	Dispositions juridiques et expérience pratique	Evaluation
	Demandes internationales (article 30 de la Convention de Budapest) : La divulgation partielle de données de trafic et d'inscription (dont celles nécessaires pour identifier la trajectoire d'une communication au sens de l'article 30 de la Convention de Budapest) peut être effectuée sur demande d'entraide judiciaire. Cependant, si le prestataire amont ne se trouve pas aux Etats-Unis, les autorités répressives étasuniennes signalent le pays et le prestataire aux autorités requérantes étrangères. En outre, si les autorités répressives étasuniennes constatent de leur côté – par exemple en ouvrant leur propre enquête – qu'une adresse IP ou un nom de domaine ne se trouve pas aux Etats-Unis, ces informations peuvent être transmises aux autorités étrangères. Cette disposition n'est pas beaucoup utilisée en pratique.	supposent une demande d'entraide judiciaire.

4 Préservation rapide et conservation des données

4.1 Une clarification nécessaire

Il ressort de certaines réponses au questionnaire du T-CY et des échanges avec les personnes concernées, en Europe et ailleurs, que les notions de « préservation » et de « conservation » des données ne sont pas toujours bien comprises.

4.1.1 Préservation rapide

Les articles 16 et 30 de la Convention de Budapest sur la cybercriminalité demandent aux Parties d'adopter des mesures pour rendre possible la préservation rapide[9] de données informatiques spécifiées, au niveau national et international.

Ainsi, les autorités répressives doivent être en mesure d'ordonner à un prestataire de services ou à toute autre personne physique ou morale de préserver toute donnée spécifiée (relative au trafic, au contenu ou à la personne inscrite) susceptible de servir de preuve dans le cadre d'une enquête précise. La préservation porte sur les données stockées, c'est-à-dire déjà existantes, et non sur des données à venir, qui appellent d'autres mesures (collecte en temps réel de données de trafic ou interception de données de contenu).

Les mesures de préservation rapide ne se limitent ni aux infractions pénales graves, ni aux infractions qui utilisent ou visent un système informatique mentionnées aux articles 2 à 10 de la Convention de Budapest. La préservation doit être possible pour les preuves électroniques liées à toute infraction pénale (article 14.2 de la Convention de Budapest).

Il s'agit d'une mesure provisoire, qui doit être applicable précocement pour assurer sans retard la préservation de données par nature éphémères[10]. Elle laisse le temps nécessaire à l'étape suivante, c'est-à-dire l'obtention proprement dite des données via les procédures formelles, comme la perquisition et saisie ou les injonctions de produire, qui requièrent dans la plupart des pays un mandat judiciaire.

La mesure provisoire de préservation des données est particulièrement importante pour la coopération internationale, puisque les perquisitions et saisies ou les injonctions de produire ne sont le plus souvent possibles qu'après réception d'une demande formelle d'entraide judiciaire de la part de l'Etat étranger requérant.

La Convention de Budapest sur la cybercriminalité ne couvre pas le concept de conservation des données.

4.1.2 Conservation des données

Beaucoup de Parties ont adopté une réglementation sur la conservation des données, notamment sur la base de la directive adoptée en 2006 à ce sujet par l'Union européenne[11]. Les gouvernements de

---

[9] En anglais « *expedited preservation* ». Dans le texte français de la Convention de Budapest : « conservation rapide ». Voir note de la traductrice au début du présent document.

[10] La préservation rapide est parfois appelée « gel rapide », bien que le terme puisse prêter à confusion.

[11] « Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE ». Pour le texte, voir : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:FR:HTML

beaucoup d'autres pays ont aussi adopté ou envisagent d'adopter des obligations de conservation des données[12].

Etat partie	Obligation de conserver les données
Albanie	Oui, deux ans
Arménie	Non
Azerbaïdjan	Non (à l'étude)
Bosnie-Herzégovine	Oui, un an
Bulgarie	Oui, un an. Les données consultées peuvent être conservées six mois de plus.
Croatie	Oui, un an
Chypre	Oui, six mois
Danemark	Oui, un an
Estonie	Oui, un an
Finlande	Oui, un an
France	Oui, un an
Allemagne	Non (loi abrogée)
Hongrie	Oui, six mois pour les appels infructueux, un an pour les autres données
Islande	Oui
Italie	Oui, vingt-neuf mois pour les données téléphoniques, six mois pour les données internet
Lettonie	Oui, dix-huit mois
Lituanie	Oui, six mois
République de Moldova	Oui, trois mois
Monténégro	Oui
Pays-Bas	Oui, un an
Norvège	Non (en attente d'entrée en vigueur)
Portugal	Oui, un an
Roumanie	Oui, six mois
Serbie	Oui, douze mois
Slovaquie	Oui, un an pour les données de téléphonie fixe et mobile, six mois pour les données internet (consultation, courrier électronique et téléphonie par internet)
Slovénie	Oui, quatorze mois pour les données téléphoniques, huit mois pour les données internet
Espagne	Oui, un an
Suisse	Oui, six mois
« L'ex-République yougoslave de Macédoine »	Oui
Ukraine	Oui, trois ans
Royaume-Uni	Oui, un an
Etats-Unis d'Amérique	Non

En vertu de la directive, toutes les données de trafic, de localisation et d'inscription liées à la téléphonie fixe et mobile, à la consultation d'internet, au courrier électronique et à la téléphonie par internet doivent être conservées « pour une durée minimale de six mois et maximale de deux ans à compter de la date de la communication » (article 6).

Pour les mesures nationales d'exécution, adoptées par les Etats membres de l'UE pour appliquer la directive, voir : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:FR:NOT

Après une évaluation menée en 2011, la directive est actuellement en cours de révision. Pour le rapport d'évaluation, voir : http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_fr.pdf

[12] Beaucoup se sont appuyés sur la directive de l'UE sur la conservation des données. On peut supposer que le résultat de la révision en cours de cette directive donnera de nouvelles orientations aux pays tiers.

Le texte ne couvre ni les données de contenu, ni les URL, ni les adresses IP des destinataires, ni les en-têtes de courriers électroniques : « [La directive] ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques » (article premier).

Il faut aussi noter que les définitions des « données de trafic » et des « fournisseurs de services » sont plus restrictives dans la directive UE que dans la Convention de Budapest[13].

La directive vise à garantir la disponibilité des données « à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque Etat membre dans son droit interne » (article premier)[14].

Les données doivent être conservées « dans la mesure où [les données] sont générées ou traitées dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'Etat membre concerné » (article 3).

L'article 7(d) précise : « les données sont détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles on a pu accéder et qui ont été préservées[15] ».

Les données sont conservées par le prestataire de services. La directive laisse aux pouvoirs publics nationaux le soin de définir dans quelles conditions les autorités de justice pénale peuvent accéder aux données conservées.

4.1.3 Des mesures complémentaires

La préservation rapide et la conservation des données sont deux notions différentes.

Les réponses au questionnaire montrent que les deux mesures sont jugées complémentaires. Elles peuvent être appliquées en parallèle, l'une après l'autre ou séparément, à des fins différentes. Par exemple :

---

[13] La directive sur la conservation des données s'applique, « dans le cadre de la fourniture des services de communication concernés », aux « fournisseurs de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'Etat membre concerné », tandis que l'article 1.c de la Convention de Budapest couvre « toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ». La directive énumère les catégories de données de trafic et de localisation à conserver, tandis que la Convention (article 1.d) donne une définition plus ouverte des données relatives au trafic.

[14] Les Etats membres de l'UE ont transposé de diverses manières cette « restriction d'objectifs ». Dans certains Etats membres, l'accès aux données conservées est possible en lien avec un plus large éventail d'infractions (comme en Belgique, au Danemark, en France, en Italie, en Lettonie, en Pologne, en Slovaquie ou en Slovénie). Les arrêts de cours constitutionnelles qui ont annulé les lois transposant la directive, en Roumanie (octobre 2009), en Allemagne (mars 2010) et en République tchèque (mars 2011), mettent en évidence la nécessité de limites et de garanties plus strictes (voir le Rapport d'évaluation concernant la directive sur la conservation des données (COM(2011)225 final), page 21
(http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_fr.pdf).

[15] Il semble que beaucoup de pays non européens aient adopté des règles de conservation des données prévoyant une durée de conservation minimale, mais sans obligation de détruire les données au bout d'un certain temps.

- L'obligation de conserver les données augmente les chances que les données de trafic, de localisation et d'inscription à préserver soient toujours disponibles.
- Si le délai de conservation automatique est sur le point d'expirer, une demande de préservation permet de sauvegarder des données spécifiées, pour une enquête précise, au-delà de cette période.
- Les données conservées ne peuvent être consultées qu'en lien avec une infraction grave, tandis que les demandes de préservation peuvent être formulées et permettre l'obtention de preuves électroniques pour tout type d'infraction. Il a été souligné que dans le cas d'une infraction informatique, la gravité de l'infraction n'est pas toujours manifeste dès le début de l'enquête[16].
- Alors que l'obligation de conserver les données concerne les prestataires de « services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'Etat membre concerné », les demandes de préservation peuvent être adressées à toute personne physique ou morale détenant des données.
- Les articles 29 et 30 de la Convention de Budapest permettent d'adresser des demandes de préservation internationales y compris aux pays qui n'imposent pas la conservation des données.

	Préservation rapide	**Conservation des données (directive)**
Objectif	Mesure provisoire destinée à préserver des preuves électroniques évanescentes, pour assurer le délai nécessaire aux mesures formelles d'obtention des preuves	Veiller à ce que les données soient disponibles pour la recherche, la détection et la poursuite d'infractions graves
Spécifié/ automatique	Demande spécifique, portant sur des données spécifiques	Conservation automatique des données
Type de données	Toute donnée (y compris de contenu)	Données de trafic, de localisation et d'inscription (les données de contenu, adresses IP des destinataires, URL, en-têtes de courriers électroniques ou listes de destinataires en copie sont exclus)
Restriction d'objectifs	Toute infraction liée à des preuves électroniques	Infractions graves
Acteurs concernés	Toute personne physique ou morale (sans restriction aux prestataires de services)	Les prestataires de services
Durée	Flexible : 90 jours (renouvelable)	Durée de conservation spécifique (6 à 24 mois, à préciser en droit interne)

La plupart des réponses indiquent donc que les deux mesures sont nécessaires.

Au niveau national, la conservation des données diminue l'intérêt des demandes de préservation, puisque les autorités de justice pénale peuvent obtenir les données de trafic, de localisation ou d'inscription conservées au moyen de perquisitions et saisies ou d'injonctions de produire sans passer par des mesures provisoires.

[16] L'enquête sur un cas de fraude apparemment mineur peut révéler les liens entre une adresse IP et une vaste opération criminelle à l'échelle internationale.

En fait, les informations disponibles indiquent que pour les données de trafic, de localisation et d'inscription, le nombre de demandes d'accès aux données conservées dépasse nettement celui des demandes de préservation. Le rapport pourrait être supérieur à mille demandes de données conservées pour une demande de préservation[17].

Les réponses suggèrent également que la mesure de préservation est largement sous-utilisée.

Ainsi, la conservation des données complète la préservation rapide mais ne la remplace pas. Bien que la conservation des données semble utile pour figer des données de trafic, de localisation et d'inscription, une Partie qui n'appliquerait que cette mesure ne respecterait pas pleinement les articles 16, 17, 29 et 30 de la Convention de Budapest.

[17] Voir les statistiques du Rapport d'évaluation concernant la directive sur la conservation des données (COM(2011)225 final) : en 2008, les demandes de données conservées ont été au nombre de 131 560 en République tchèque, 3 599 au Danemark, 12 684 en Allemagne, 14 095 en Irlande, 53 578 en Espagne, 503 437 en France, 16 892 en Lettonie, 85 315 en Lituanie, 869 à Malte, 85 000 aux Pays-Bas et 470 222 au Royaume-Uni. Comme indiqué, plusieurs Etats membres de l'UE ne limitent pas l'accès aux données conservées aux infractions graves. Ces chiffres doivent être pris avec précaution, puisqu'ils reflètent l'accès à différents types de données selon des règles différentes.

5 Conclusions

Le présent rapport a été débattu par le T-CY lors de sa 7e réunion plénière (juin 2012) et adopté lors de sa 8e réunion plénière (décembre 2012[18]). Il évalue la mise en œuvre par les Parties de quatre articles de la Convention de Budapest sur la cybercriminalité :

- Article 16 – Préservation rapide de données informatiques stockées (niveau national)
- Article 17 – Préservation et divulgation rapides de données relatives au trafic (niveau national)
- Article 29 – Préservation rapide de données informatiques stockées (niveau international)
- Article 30 – Divulgation rapide de données préservées (niveau international).

5.1 Conclusions et recommandations

Le T-CY

- considère que l'évaluation de l'application de dispositions spécifiques de la Convention de Budapest renforcera l'efficacité de la Convention ;
- se félicite que 31 Etats parties aient répondu au questionnaire du T-CY et participé à l'évaluation ;
- regrette de ne pas avoir reçu de réponse du Danemark et de l'Islande ;
- appelle toutes les Parties à participer activement aux évaluations futures, dans l'intérêt de l'efficacité de la Convention de Budapest et d'une bonne coopération internationale contre la cybercriminalité.

Le T-CY adopte les conclusions et recommandations générales suivantes :

1. Les dispositions de la Convention de Budapest sur la préservation rapide, notamment ses articles 16 et 29, constituent de très précieux outils pour figer des preuves par nature évanescentes dans un contexte international. La préservation rapide de preuves électroniques assure le délai nécessaire au dépôt de demandes formelles d'entraide judiciaire.

2. Plusieurs Parties ont adopté des dispositions juridiques spécifiques, conformément aux articles 16, 17, 29 et 30.

3. De très nombreux Etats parties s'appuient sur des pouvoirs généraux, sur des perquisitions et saisies ou sur des injonctions de produire, souvent en combinaison avec la conservation des données, pour préserver rapidement des preuves électroniques. Certains semblent ainsi en mesure de remplir la plupart des exigences énoncées aux articles 16, 17, 29 et 30.

4. Cependant, ces pouvoirs ne peuvent toujours remplacer la préservation, en particulier dans le cas de demandes internationales. Il peut être plus difficile et plus long d'obtenir des

[18] À sa 8e réunion plénière, le T-CY a adopté le rapport d'évaluation en principe, dans l'attente d'informations supplémentaires à fournir par certaines Parties. Le rapport a été adopté par procédure écrite le 25 janvier 2013.

perquisitions et saisies ou des injonctions de produire, puisqu'elles sont assorties de garanties plus strictes que la préservation (article 15 Convention de Budapest) ou peuvent être détectées par le suspect.

5. Par ailleurs, une plus grande sécurité juridique entourant les demandes de préservation pourrait aider à améliorer la coopération entre les autorités répressives et les prestataires de services. Recommandation : Même si les mécanismes actuels permettent de figer rapidement des preuves électroniques, les Parties devraient envisager l'adoption de dispositions spécifiques dans leur droit interne. La législation devrait imposer aux prestataires de services et aux autres personnes physiques ou morales devant préserver des données de garder le secret sur cette opération.

6. Le T-CY souligne en particulier que la préservation et la conservation des données peuvent constituer des outils complémentaires mais poursuivent des objectifs différents, et que la conservation des données ne peut donc se substituer à la préservation.

7. Le T-CY note que dans plusieurs Etats parties, les conditions d'accès aux données conservées sont telles que les données de trafic sont plus difficiles à obtenir que les données de contenu, pourtant plus sensibles au regard de la vie privée.

8. Certaines Parties ne sont pas en mesure de préserver ou de figer rapidement des preuves électroniques et ne respectent donc pas les articles de la Convention de Budapest à ce sujet. Recommandation : Ces Parties sont encouragées à prendre des mesures urgentes pour permettre à leurs autorités compétentes de préserver des preuves électroniques dans le cadre de procédures nationales et internationales.

9. Les pouvoirs de préservation sont largement sous-utilisés, alors que les réponses au questionnaire confirment leur importance. Recommandation : Les Parties devraient prendre les mesures appropriées pour accroître l'utilisation de ces pouvoirs par les autorités compétentes. Ces mesures peuvent englober des formations et des orientations sur l'usage des pouvoirs de préservation à l'attention des autorités répressives. Cela vaut aussi pour les articles 17 et 30, sur la divulgation partielle de données de trafic.

10. Les points de contact 24/7 mis en place en vertu de l'article 35 de la Convention de Budapest constituent un moyen concret d'envoyer et de recevoir des demandes de préservation (articles 29 et 30). Les réponses au questionnaire laissent penser qu'ils ne sont pas beaucoup mis à contribution. Recommandation : Les Parties devraient agir pour informer toutes les autorités nationales de la possibilité d'utiliser les points de contact 24/7 pour une coopération internationale urgente sur les questions liées à la cybercriminalité et aux preuves électroniques.

11. Le T-CY note que le recours limité aux mesures provisoires des articles 29 et 30 tient en partie à la complexité de la procédure d'entraide judiciaire qui doit suivre. Recommandation : Le T-CY devrait consacrer son prochain cycle d'évaluation (en 2013) à l'article 31, « Entraide concernant l'accès aux données stockées ».

5.2 Synthèse de l'application des articles par les Parties

Etat partie (O = conforme P = Partiellement conforme N = non conforme à la Convention de Budapest)	**Article 16 Préservation rapide**	**Article 29 Préservation rapide (international)**	**Article 17 Préservation et divulgation partielle**	**Article 30 Préservation et divulgation partielle (international)**
1. Albanie	O	O	O	O
2. Arménie	N	N	N	N
3. Azerbaïdjan	P	P	O	O
4. Bosnie-Herzégovine	P	P	P	P
5. Bulgarie	O	O	O	O
6. Croatie	O	O	O	O
7. Chypre	P	P	P	N
8. Danemark	Pas d'information	Pas d'information	Pas d'information	Pas d'information
9. Estonie	P	P	P	P
10. Finlande	O	O	O	O
11. France	O	O	O	O
12. Géorgie	P	P	P	P
13. Allemagne	O	O	P	P
14. Hongrie	O	P	P	N
15. Islande	Pas d'information	Pas d'information	Pas d'information	Pas d'information
16. Italie	O		O	O
17. Lettonie	O	O	O	O
18. Lituanie	P	P	P	P
19. République de Moldova	P	O	O	O
20. Monténégro	O	O	P	P
21. Pays-Bas	O	O	O	O
22. Norvège	O	O	O	O
23. Portugal	O	O	O	O
24. Roumanie	O	O	O	O
25. Serbie	O	O	O	O
26. Slovaquie	O	O	Pas d'information	Pas d'information
27. Slovénie	P	P	P	P
28. Espagne	N	N	N	N
29. Suisse	O	O	O	Pas d'information
30. « L'ex-République yougoslave de Macédoine »	O	O	P	P
31. Ukraine	N	N	N	N
32. Royaume-Uni	O	O	O	O
33. Etats-Unis d'Amérique	O	O	O	O

5.3 Suivi

Les Parties sont invitées à informer à tout moment le Secrétariat des mesures qu'elles ont prises et de leurs exemples de bonnes pratiques.

Le T-CY fera le point sur les progrès accomplis dans les dix-huit mois suivant l'adoption du rapport (c'est-à-dire mi-2014).

6 Appendix 1: Domestic legal provisions on expedited preservation[19]

6.1 Albania

Expedited preservation:

Article 299/a Criminal Procedure Code
Expedited preservation and maintenance of the computer data
1. the prosecutor may order the expeditious preservation of certain computer data, including traffic data, when there are enough reasons to believe that the data may be lost, damaged or altered.
2. If the computer data is in the possession or control of a person, the prosecutor can order this person to preserve and maintain the integrity of the specified computer data for a period of up to 90 days, in order to search and disclose them. When there are reasonable grounds, this timeframe can be renewed only once.
3. The person in charge of preserving and maintaining the computer data is obliged to keep confidential the procedures and actions undertaken under point 2 of this article until the end of investigations.

Law no. 9918 dated 19.05.2008 "On electronic communication"
Article 101 "Preservation and administration of data for the purpose of
criminal prosecution"
1. Regardless of other definitions in this law, the operators of networks and public electronic communications are obliged to preserve and administer the data records of their subscribers for a period of two years.
2. These records should contain data that enable:
a) The identification of subscribers ensuring the registration of their full identity
b) The identification of the end equipment used in the communication
c) the identification of the date, hour, duration of communication and the number called
3. These records should be made available, also in an electronic form, to the authorities referred to in the Criminal Procedure Code, based upon their request

Partial disclosure:

Article 299/b Criminal Procedure Code
Expedited preservation and partial disclosure of computer data
The person in charge of expeditious preservation and maintain ace of the traffic data is obliged to undertake all the necessary measures to ensure that the stored data is valid, regardless of whether one or more service providers were involved in the transmission of the communication as well as to provide the prosecutor or the authorized judicial police officer with a sufficient amount of traffic data to enable the identification of the service provider and the path through which the communication was transmitted

6.2 Bosnia and Herzegovina

No specific legal provision. Use production order:

CPC BiH - ART. 72a
Order to the telecommunications operator

[19] Based on replies to questionnaire and/or Country Profiles at www.coe.int/cybercrime

(1)If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.
(2)In case of emergency, the Prosecutor may order the measures under Paragraph (1) of this Article, in which case the information received shall be sealed until the issuance of the court order. The Prosecutor shall immediately inform the preliminary proceedings judge, who may issue an order within 72 hours. In case the preliminary proceedings judge does not issue the order, the Prosecutor shall return such information unsealed.
(3)Measures under Paragraph (1) of this Article may also be ordered against a person if there are grounds for suspicion that he will deliver to the perpetrator or will receive from the perpetrator information related to the offence, or grounds for suspicion that the perpetrator uses a telecommunication device belonging to this person.
(4)Telecommunications operators or other legal persons who provide telecommunications services shall enable the Prosecutor and police authorities to enforce the measures referred to in Paragraph (1) of this Article.

Similar provisions are available at entity level (CPC of RS, Art. 137 and CPC of Federation, Art. 86a).

6.3 Bulgaria

[extract from country profile 2011]

Art. 125, Art. 159, Art.162 (6), Art.163, Art. 172 (3) PPC
Chapter fourteen TECHNIQUES FOR ESTABLISHING EVIDENCE

Section III. Types of objective forms of evidence
Preparation and attachment to the case file of material evidence Article 125 (1) Where material evidence cannot be separated from the place, where it was found, and also in other cases specified by this Code, the following shall be prepared: photographs, slides, films, video tapes, sound-recordings, recordings on carriers of computerized data, layouts, schemes, casts or prints thereof.
(2) The court and the authorities entrusted with pre-trial proceedings shall also collect and inspect the objective forms of evidence prepared with the use of special intelligence means in the hypotheses herein set forth.
(3) The materials under the paragraphs 1 and 2 shall be enclosed with the case file.
Persons who shall prepare objective forms of material evidence

Section V.Searches and seizures

Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data
Article 159 Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Persons present in the course of searches and seizures
Article 162 (6) Where searches and seizures concern computerized information systems and software applications, these shall be conducted in presence of an expert- technical assistant.

Conducting searches and seizures

Article 163 (1) Searches and seizures shall be performed in daytime, except where they can suffer no delay.

(2) Before proceeding with a search and seizure, the respective body shall submit the authorisation therefore, and shall ask the objects, papers, and computerized information systems containing computerized data sought to be shown to him/her.

6.4 Croatia

Expedited preservation:

Criminal Procedure Act (Official Gazette 152/08, 76/09, 80/11)
Temporary Seizure of Objects

Article 261

(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.

(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.

(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.

(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 263

(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider, except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.

(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case handing over is denied, it may be pursued in accordance with Article 259 paragraph 1 of this Act.

(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the obligation to observe confidentiality (Articles 186 to 188) during acquiring, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against which the measure is applied, may be recorded to appropriate device and be returned to this person even prior to the conclusion of the proceedings.

(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, as long as necessary and six months at longest. After this term data shall be returned, unless:

1) they are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a) and computer fraud (Article 224a);

2) they are related to committing another criminal offence which is subject to public prosecution, committed by using a computer system;
3) they are not used as evidence of a criminal offence for which proceedings are instituted.

(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.
According to article 213. of CPA there is also possibility of evidence collecting actions before commencement of proceedings;

Article 213.

(1) The State Attorney, or the investigator upon his order, may before the commencement of the investigation, when the investigation is mandatory (Article 216 paragraph 1), conduct evidence collecting actions for which there is danger in delay, and the police may temporarily seize the items referred to in Article 261 of this Act when conducting investigation of criminal offences.

(2) If the investigation according to this Act is not mandatory, the State Attorney or the investigator upon his order, may carry out evidence collecting actions for which there is danger in delay or that are purposeful for deciding on preferring the indictment.

(3) In the case from paragraph 2 of this Article, and after receiving the instruction on the rights (Article 239), the suspect may propose evidence collecting actions to the State Attorney, and the conduct of an evidentiary hearing to the investigating judge in the cases referred to in Article 236 paragraph 2 of this Act.

(4) If a criminal charge has been filed against the defendant or he has been searched, or his home and other areas he uses and mobile objects he uses have been searched, or if an object has been temporarily confiscated from the suspect, identification conducted or fingerprints taken or prints of other body parts of the suspect, or a sample of biological material, or if an expertise of the suspect was ordered pursuant to Article 325 or 326 of this Act, the defendant may apply for the first investigation with the state attorney within 30 days from the day when criminal charge was filed or the suspect has been searched, or his home or other areas he uses or movable objects he/she uses have been searched or objects have been temporarily confiscated from the suspect, suspect identification conducted or fingerprints or prints of other body parts of the suspect taken, biological material samples taken or suspect expertise ordered pursuant to Articles 325 or 326 of this Act. If the state attorney should accept the suspect's proposal, he shall be interrogated within that term.

(5) If the state attorney has not interrogated the suspect within the term from paragraph 4 of this Article, the suspect shall have the right to review the deed upon the expiry of that term.

Special Collection of Evidence

Article 332

(1) If the investigation cannot be carried out in any other way or would be accompanied by great difficulties, the investigating judge may, upon the written request with a statement of reasons of the State attorney, order against the person against whom there are grounds for suspicion the he committed or has taken part in committing an offence referred to in Article 334 of this Act, measures which temporarily restrict certain constitutional rights of citizens as follows:

1) surveillance and interception of telephone conversations and other means of remote technical communication;

2) interception, gathering and recording of electronic data;

3) entry on the premises for the purpose of conducting surveillance and technical recording at the premises;

4) covert following and technical recording of individuals and objects;

5) use of undercover investigators and informants;

6) simulated sales and purchase of certain objects, simulated bribe-giving and simulated bribe-taking;

7) offering simulated business services or closing simulated legal business;

8) controlled transport and delivery of objects from criminal offences.

Article 333
(1) Recordings, documents and objects obtained by the application of the measures referred to in Article 332 paragraph 1 item 1 to 8 of this Act may be used as evidence in criminal proceedings.

Furthermore, Article 336 Paragraph 2. of the CPC, requires all persons who are in any way to learn about the content or actions of persons involved in implementing the actions referred to in Article 332. (Special collection of evidence), that they must keep that information secret.

Also, the CPC has a general provision on confidentiality of the investigation (Article231).

Partial disclosure:

Criminal Procedure Act (Official Gazette 152/08, 76/09, 80/11);

Article 335. par. 2.
(2) The technical operation centre for the supervision of telecommunications that carries out technical coordination with the provider of telecommunication services in the Republic of Croatia as well as providers of telecommunication services shall be bound to provide the necessary technical assistance to the police authorities. In case of proceeding contrary to this obligation, the investigating judge shall upon the motion with a statement of reasons of the State Attorney impose a fine on a provider of telecommunication services in an amount of up to HRK 1,000,000.00, and on a responsible person in the technical operative centre for the supervision of telecommunications that carries out technical coordination and on a provider of telecommunication services in the Republic of Croatia in an amount of up to HRK 50,000.00, and if thereafter the ruling is not complied with, the responsible person may be punished by imprisonment until the ruling is executed, but not longer than one month. The panel shall decide on the appeal against the ruling on the fine and imprisonment. The appeal against the ruling on the fine and imprisonment shall not stay its execution.

Decree on obligations from the area of national security of the Republic of Croatia for legal and physical persons in telecommunications (Official Gazette 64/08).

Electronic Communication Act (OG 73/08, 90/11)

6.5 Estonia

Preservation is covered by the general powers of police and prosecutor of the Criminal Procedure Code.

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices

(1) The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

For data retention:

Electronic Communications Act

§ 111₁. Obligation to preserve data

(1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts:

1) tracing and identification of the source of communication;

2) identification of the destination of communication;

3) identification of the date, time and duration of communication;

4) identification of the type of communications service;

5) identification of the terminal equipment or presumable terminal equipment of a user of communications services; 6) determining of the location of the terminal equipment.

(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:

1) the number of the caller and the subscriber's name and address;

2) the number of the recipient and the subscriber's name and address;

3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;

4) the date and time of the beginning and end of the call;

5) the telephone or mobile telephone service used;

6) the international mobile subscriber identity (IMSI) of the caller and the recipient;

7) the international mobile equipment identity (IMEI) of the caller and the recipient;

8) the cell ID at the time of setting up the call;

9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;

10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

(3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data:

1) the user IDs allocated by the communications undertaking;

2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;

3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

4) the user ID or telephone number of the intended recipient of an Internet telephony call; 5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;

6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID; 7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;

8) the Internet service used in the case of electronic mail and Internet telephony services; 9) the number of the caller in the case of dial-up Internet access;

10) the digital subscriber line (DSL) or other end point of the originator of the communication.

(4) The data specified in subsections (2) and (3) of this section shall be preserved for one year from the date of the communication if such data are generated or processed in the process of provision of communications services. Requests submitted and information given pursuant to § 112 of this Act shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 rests with the person submitting the request.

(5) The data specified in subsections (2) and (3) of this section shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia: 1) the requests and information provided for in § 112 of this Act;

2) the log files specified in subsection 113 (5) and the applications provided for in subsection 113 (6) of this Act; 3) the single requests provided for in § 1141 of this Act.
(6) In the interest of public order and national security the Government of the Republic may extend, for a limited period, the term specified in subsection (4) of this section.
(7) In the case specified in subsection (6) of this section the Minister of Economic Affairs and Communications shall immediately notify the European Commission and the Member States of the European Union thereof. In the absence of an opinion of the European Commission within a period of six months the term specified in subsection (4) shall be deemed to have been extended.
(8) The obligation to preserve the data provided for in subsections (2) and (3) of this section also applies to unsuccessful calls if those data are generated or processed upon providing telephone or mobile telephone services or telephone network or mobile telephone network services. The specified obligation to preserve data does not apply to call attempts.
(9) Upon preserving the data specified in subsections (2) and (3) of this section, a communications undertaking must ensure that:
1) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network;
2) the data are protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;
3) necessary technical and organisational measures are in place to restrict access to the data; 4) no data revealing the content of the communication are preserved.
(10) The expenses related to the preserving or processing of the data specified in subsections (2) and (3) of this section shall not be compensated to communications undertakings.
(11) The data specified in subsections (2) and (3) of this section are forwarded only to a surveillance agency, a security authority, the Financial Supervision Authority or a court pursuant to the procedure provided by law.

§ 112. Obligation to provide information to surveillance agency and security authority
(1) If a surveillance agency or security authority submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than 10 hours after receiving an urgent request or within 10 working days if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the surveillance agency or security authority with information concerning the data specified in subsections 1111 (2) and (3) of this Act.
(2) The request specified in subsection (1) of this section shall be submitted in writing or by electronic means. Requests concerning the data specified in clauses 1111(2) 1) and 2) and clause 1111 (3) 3) of the Act may also be submitted in oral form confirming the request with a password. Access to the data specified in subsection (1) of this section may be ensured, on the basis of a written contract, by way of continuous electronic connection.
(3) A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority with real time identification of the location of the terminal equipment used in the mobile telephone network.
(4) Access to the data specified in subsection (3) of this section must be ensured on the basis of a written contract and by way of continuous electronic connection.

6.6 Finland

Budapest Convention has been implemented using similar procedure as is used with all other international conventions in Finland. This means enacting a so called "blanco" legislation (539/2007) which in a nutshell states that provisions of this convention which belong to the sphere of law in Finland are, in a manner Finland has bound itself to, in force as a law in Finland. In addition to this blanco provision also some additional provisions has been introduced into Finnish legislation. As regards article 16, the relevant national provisions which were introduced due to implementation of Budapest Convention were included in to Coercive measures Act (450/1987). Chapter 4 section 4b includes a provision on data preservation order and article 4c on duration of the data preservation

order and on confidentiality. With these provisions Finnish legislation complies with articles 16 and 17 of the Convention. Unfortunately there is no English translation of these provisions (content of provisions is explained below).

The content of those provisions in essence is that (4b) If there is reason to assume that data which might have relevance in order to investigate an offence concerned will be lost or altered, an official having the competence to order an arrest may order a person holding the data to keep it unaltered. This does not apply to suspected person. A written certificate must be provided on request. These rules apply also to traffic data. Based on this preservation order, the authority does not have the right to get the information regarding the content of the data. If several service providers are involved, then the authority has the right to get the necessary traffic information in order to identify the service providers.

According to 4c, the data preservation order is ordered for fixed period of time for maximum of 3 months at a time. If the investigation requires, this period may be prolonged for maximum 3 months at a time. Person who has received the preservation order is obliged to keep it confidential. For breaching this obligation of confidentiality the penalties of chapter 38 article 1 or 2 of the criminal code applies unless a more severe punishment is provided for elsewhere in legislation.

After total reform of Coercive measures Act, these provisions on data preservation order are included in "new" Coercive measures Act (806/2011) Chapter 8, sections 24-26.

6.7 France

Pour ART. 16 (1)- ART. 56, paragraphe 7 du Code de Procédure Pénale
Avec l'accord du procureur de la République, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité.
Le procureur de la République peut également, lorsque la saisie porte sur des espèces, lingots, effets ou valeurs dont la conservation en nature n'est pas nécessaire à la manifestation de la vérité ou à la sauvegarde des droits des personnes intéressées, autoriser leur dépôt à la Caisse des dépôts et consignations ou à la Banque de France.

ART. 60-2 du Code de Procédure Pénale, voir paragraphe 2.
L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant exceeder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.
Preservation and retention forseen in different other laws and regulations:

- loi « informatique et liberté » de janvier 1978
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=3&fastReqId=34057747&categorieLien=cid&oldAction=rechTexte

- loi sur la sécurité quotidienne du 15/11/2001, art 29
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&fastPos=3&fastReqId=61552634&categorieLien=id&oldAction=rechTexte

- loi pour la confiance dans l'économie numérique de 2004, art 6
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&fastPos=5&fastReqId=347283023&categorieLien=id&oldAction=rechTexte

- décret n°2006-358 du 24 mars 2006

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&fastPos=3&fastReqId=134 42746&categorieLien=id&oldAction=rechTexte

- décret n°2011-219 du 25 février 2011

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&fastPos=1&fastReqId=134 42746&categorieLien=id&oldAction=rechTexte

6.8 Germany

German Code of Criminal Procedure (Strafprozessordnung), 2008 ("StPO"):
With respect to computer data, Article 16 is covered by Sections 94, 95 and 98 StPO.

Section 94
[Objects Which May Be Seized]
(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95
[Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 98
[Order of Seizure]
(1) Seizure may be ordered only by the judge and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a judicial order shall apply for judicial approval within 3 days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a judicial decision. As long as no public charges have been preferred, the decision shall be made by the court of competency pursuant to Section 162 subsection (1). Once public charges have been preferred, the decision shall be made by the court dealing with the matter. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.
(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within 3 days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.
With respect to traffic data, Article 16 is covered by Section 100g StPO.

Section 100g
[Information on Telecommunications Connections]

(1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory,
1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or
2. has committed a criminal offence by means of telecommunication;
then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.
(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply mutatis mutandis. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.
(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.
(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying:

1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.

Section 100a
[Conditions regarding Interception of Telecommunications]
(1) […]
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.

Section 100b
[Order to Intercept Telecommunications]
(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.
(2) The order shall be given in writing. The operative part of the order shall indicate:
1. where known, the name and address of the person against whom the measure is directed,

2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.
(3) On the basis of this order all persons providing, or contributing to the provision
of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply mutatis mutandis.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) […]

6.9 Georgia

Article 111. General Rule for Conducting Investigative Actions
1. The parties have equal rights and obligations during the conduct of investigative actions according to the rule established by this Code except the cases determined under paragraph 2 of this article. The parties conduct investigative actions according to the rule established by this Code and within its frames. A prosecutor is authorized to attend the investigative action conducted by the law enforcement institutions. The law enforcement institutions shall not conduct investigative actions without the participation of a prosecutor if he/she demands so. A prosecutor shall be entitled to be present at the investigative action carried out by the defense, with the consent of the defense.
2. A defense is not authorized to submit a motion to a court for conduct of search and seizure.
3. Prior to launching an investigative action, a person carrying out an investigative action shall explain to the participants their rights and duties, and the rules for conducting an investigative action. The person conducting an investigative action is required to ensure that the involved parties have opportunity to exercise their rights.
4. If an investigator's ruling or a court order authorizes an investigative action, the investigator shall under signature present the ruling (court order) to the person required to fulfill it.
5. It shall be impermissible to carry out the investigative action at night, except in cases of urgency. An investigative action shall be conducted within a reasonable time.
6. Scientific-technical means and methods for discovering, securing, and extracting trace evidence and physical evidence may be used during investigative action.
7. In case of resistance toward an investigative action, a proportionate compulsory measure may be applied.
8. During an investigative action, it shall only be permissible to apply surgical, or other methods and means of medical examination, that cause considerable pain, in exceptional cases , with the consent of a person to be examined; if a person to be examined is under 16 years of age or he/she is mentally ill, with the consent of a parent, guardian or custodian, or by a court order.
9. If a conduct of an investigative activity requires special professional skills, a party shall conduct it with participation of an expert. If an investigative activity requires that an individual to be undressed, upon to the his/her request, an expert and a party shall be of the same sex as the person under examination.

Article 112. Investigative Action Conducted on the Basis of a Court Order
1. An investigative action related to the restriction of one's private property, ownership or right to privacy of a dwelling, shall be carried out on the basis of a court order issued on the motion of the parties. A judge shall without the oral hearing decide on the motion within 24 hours from the moment

of receiving a motion and other necessary information for reviewing the motion. A judge shall be authorized to consider the motion with participation of the party filing the motion. In this case rules for considering motions set forth in Article 206 of this Code shall apply. Consent of co-owner or one party to communication is sufficient to conduct investigative actions without the court order determined under this paragraph.
2. The court order shall contain the date and the place of its drafting, the last name of the judge, the person filing a motion, the order to carry out an investigative action, indicating its purpose and addressee, the term of the order's validity, a person or a body required to fulfill the order, and the judge's signature (including electronic signature). (2011.05.05)
3. The court order concerning search or seizure shall also indicate: the movable and immovable property, where the investigative action shall be permitted and person who owns it (if such person is identified), a natural person to be searched; an item, thing, substance, or any other object likely to be uncovered and seized during the search and seizure and its general characteristics; the right to apply an appropriate compulsory measure in case of resistance. A court order on search or seizure shall be invalid if such investigative action has not commenced within 30 days.
4. The order concerning arrest and seizure of a postal-telegraphic message made through the technical means of communication shall also include: the name and surname of the recipient of a message; the name, surname, and address of a person sending a message (if such information is available); a type of postal-telegraphic message to be arrested; the term of arrest; a title of a postal-telegraphic institution required to arrest a postal-telegraphic message; and the right of an investigator to examine and seize the postal-telegraphic message.
5. The investigative action referred to in Paragraph 1 of this article may be conducted without a court order, upon an investigator's ruling, in case of urgency, where delay may cause the destruction of factual data essential for the case or will make it impossible to obtain such data, or when an object, document, substance or any other object containing information is discovered during another investigative action (plain view concept), or when a real threat to a person's health or life exists. In this case a prosecutor shall notify a judge, having jurisdiction over the territory where the investigative action has been carried out, or a judge having jurisdiction over the place of investigation, within 24 hours from the moment of starting an investigative activity and shall transfer a file or a criminal case (or copies thereof) that justify the necessity of taking urgent investigative actions. A judge shall make a decision on a motion without an oral hearing within 24 hours from receiving the materials. The judge shall be authorized to consider a motion with participation of the parties (if the criminal prosecution has begun), as well as with participation of the person, against whom the investigative action has been conducted. While considering a motion a judge shall probe the legitimacy of the investigative action carried out without a court decision. A judge shall be authorized to summon a person who conducted the investigative action without a court order for obtaining explanations from the person. In this case rules for considering motions set forth in Article 206 of this Code shall apply.
6. After examining the case materials a court shall render an order on:
a) finding the investigative action legitimate;
b) finding the investigative action illegitimate and the collected information to be inadmissible evidence.
7. The judge has the right to consider the matters under this Article without an oral hearing.
8. The order issued pursuant to this article may be appealed in accordance with the rules set forth in the article 207 of this Code. The term for appeal shall be calculated from the enforcement of an order.

Article 119. The Purpose and Grounds for Search and Seizure
1. If there is a probable cause, a search and seizure shall aim at uncovering and seizure of any object, document, substance, or other item that contains information related to the case.
2. It is also permissible to conduct a search for a fugitive and/or for recovery of a corpse.
3. An object, document, or other item including information relevant to the case may be seized if a there is a probable cause that the object, document, or other item is kept in a certain place, with a certain person, and if it is not necessary to search for them.

4. It shall be possible to conduct a search for a seizure of an object, document, or other item including information relevant to a certain case, if there is a probable cause, that it is kept in a certain place, with a certain person, and if search is necessary for discovering it.

Article 120. The Rule for Search and Seizure

1. On the basis of a court order or in case of urgency – on the basis of ruling – authorizing search or seizure, an investigator shall have the right to enter storage, dwelling, or other ownership for the discovery and seizure of an object, document, or other item containing relevant information for the case.
2. Prior to a search or a seizure the investigator shall be obliged to present a court order or in case of urgency – a ruling, to a person subject to search and seizure. The presentation of the order (ruling) shall be confirmed by the signature of the person.
3. While the search/seizure is being conducted, an investigator shall have the right to restrict the person(s) at the place of search/seizure from leaving and from communicating with one another or with other persons. This shall be reflected in the relevant record.
4. Upon presenting a court order, in case of urgency – ruling, the investigator shall offer the person subject to search or seizure to voluntarily turn over the object, document, or other item containing relevant information. If the item to be seized is voluntarily turned over, it shall be noted in the record; in case of refusal to turn over the requested items voluntarily or in case of partial disclosure the seizure by coercion shall take place.
5. During the search the object, document, substance, or other item containing information, which is indicated in the court order or ruling shall be searched for and seized. Any other object containing information that might have an evidentiary value on the concerned case or that might clearly indicate on other crime, as well as the objects, substances and/or other items removed from the circulation may also be seized.
6. All items containing information, all objects, documents, substances, or other relevant items discovered during the search or seizure shall be presented to the persons participating in the investigative action if possible prior to the seizure. Upon the presentation, they shall be seized, described in detail, sealed, and packaged, if possible. Apart from the seal, the packaged items shall reflect the date and signatures of the persons participating in the investigative action.
7. During the search and seizure the investigator shall have the right to open a closed storage or premise if the person to be searched refuses to do so voluntarily.
8. If there is a probable cause that the persons present at the place of search or seizure have hidden the object, document, substance, or other item to be seized, personal search of such person shall be allowed. Such case shall be regarded as urgent necessity and, shall be conducted without a court order or a investigator's ruling. The legitimacy of search and/or seizure shall be reviewed by the court in accordance with the rules established by this Code.
9. Search or seizure in the building of a legal entity or an administrative body shall take place in the presence of the head or a representative of that entity or the body.

Article 136. Request for document or information

1. If there is a probable cause that the information or document important for the criminal case is kept in a computer system or data storage, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting relevant information or document.
2. If there is a probable cause that a person commits a crime though a computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting a service provider to submit existed subscriber information.
3. For the purpose of this Article, subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be determined:

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
4. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article 112 of the present Code.

Law of Georgia on Operative-Investigative Activity

Article 7. Definition of Operative-Investigative Activity
1. Operative-Investigative Activity is an activity of the authorized public agency or an official determined by the Law, who ensures performance of the goals provided by Article 2 of the present Law within its competence.
2. For the performance of these goals an authorized public agencies openly or through preserving conspiracy rules use:
[…]
h) Hidden recording of or eavesdropping on telephone conversation, receiving information and fixing from transmission lines (though connection to transmission means, computer networks, streamline communication), from computer system (directly or remotely) and for this purpose installation of relevant software devices; control of postal and telegraphic parcels (except diplomatic post) based on the order of the court.
[…]

6.10 Hungary

Criminal Procedure Act

ORDER TO RESERVE COMPUTER DATA

Section 158/A (1) Compulsion to reserve data means the temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by a computer system (hereinafter: computer data) over specific computer data, in order to investigate and prove a criminal offence.
(2) The court, the prosecutor or the investigating authority shall order the reservation of computer data constituting a means of evidence or required to trace any means of evidence or the establishment of the identity or location of a suspect.
(3) From the time of being notified of the order, the obliged party shall reserve the data recorded by the computer system designated in the order, and ensure its safe storage, if necessary, separately from other data files. The obliged party shall prevent the modification, deletion, destruction of the computer data, as well as the transmission and unauthorised copying thereof and unauthorised access thereto.
(4) The party ordering the reservation of data may affix its advanced electronic signature on the data to be reserved. If the reservation of the data at its original location considerably hindered the activity of the obliged party to process, manage, store or transmit data, the obliged party may, with the permission of the issuer of the order, ensure reservation by copying the data into another data medium or computer system. After the copy has been made, the issuer of the order may wholly or partially relieve the restrictions concerning the data medium and computer system holding the original data.
(5) While the measure is in effect, the data to be reserved may solely be accessed by the court, prosecutor or investigating authority having issued the order, and – with their respective permission –

the person possessing or managing the data. The person possessing or managing the data to be reserved may only provide information of such data with the express permission of the issuer of the order during the effect of the measure.
(6) The obliged party shall forthwith notify the issuer of the order if the data to be reserved has been modified, deleted, copied, transmitted or viewed without authorisation, or an indication of an attempt of the above has been observed.
(7) After issuing the order for reservation, the issuer shall start to review the affected data without delay, and depending on its findings, and either order the seizure of the data by copying them to the computer system or other data medium, or terminate the order for their reservation.
(8) The obligation to reserve data shall be in effect until the seizure of the data, but no longer than for three months. The obligation to reserve the data shall terminate if the criminal proceeding has been concluded. The obliged party shall be advised of the conclusion of the criminal proceeding. 95

6.11 Italy

Art. 132, paragraph 4ter and 4quater D. Lgs. 196/2003 (Data Protection Act)

Art. 132. Conservazione di dati di traffico per altre finalità 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonchè gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.
[Internet translation only: Art. 132. Preservation of traffic data for other purposes 4-ter. The Minister of the Interior or his delegate, on the central offices responsible for specialized computer or telematics matters of State police, the carabinieri and the guardia di finanza and the other persons referred to in paragraph 1 of article 226 of the implementing rules, coordination and transitional provisions of the code of criminal procedure, referred to in Legislative Decree July 28, 1989No. 271, they can order, including in relation to any requests made by foreign investigative authorities, operators and suppliers of services or telecommunication to preserve and protect, in accordance with the procedures laid down and for a period not exceeding ninety days, traffic data, excluding however the contents of communications, for the purpose of carrying out pre-emptive investigations provided for in article 226 of the mentioned rules laid down in Legislative Decree No. 271 of 1989— for purposes of detection and suppression of specific crimes. The measure, which may be extended, for motivated needs a total duration not exceeding six months may provide particular data storage mode and the possible unavailability of data from suppliers and operators of computer or telematic services or third parties.]

Law 28 of 18 March 2008[20]modified or introduced a range of provisional measures in the Code of Criminal Procedure, including:

Art. 244. Casi e forme delle ispezioni.

[20] This law was enacted in view of ratification of the Budapest Convention on Cybercrime by Italy.

1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)
(1) Parole aggiunte dall'art. 8, comma 1, della L. 18 marzo 2008, n. 48.

Art. 247. Casi e forme delle perquisizioni.
1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)
2. La perquisizione è disposta con decreto motivato.
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.
(1) Comma inserito dall'art 8, comma 2, della L 18 marzo 2008, n. 48

Art. 248. Richiesta di consegna.
1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.
2. Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. (1) In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.
(1) Parole così modificate dall'art. 8, comma 3, della L. 18 marzo 2008, n. 48.

Art. 254. Sequestro di corrispondenza.
1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato. (1)
2. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto.
3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.
(1) Articolo così modificato dall'art. 8, comma 3, della L 18 marzo 2008, n. 48.

Art. 254-bis. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. (1)
1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione

avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.
(1) Articolo inserito dall'art. 8, comma 5, della L 18 marzo 2008, n. 48

Art. 256. Dovere di esibizione e segreti.

1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, (1) e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.
2. Quando la dichiarazione concerne un segreto di ufficio o professionale, l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro.
3. Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il Presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.
4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.
5. Si applica la disposizione dell'articolo 204.
(1) Le parole: "*nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*" sono state inserite dall'art. 8, comma 6, della L. 18 marzo 2008, n. 48.

Art. 259. Custodia delle cose sequestrate.

1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'articolo 120.
2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. (1) Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.
(1) Periodo inserito dall'art. 8, comma 7, della L. 18 marzo 2008, n. 48.

Art. 260. Apposizione dei sigilli alle cose sequestrate. Cose deperibili.

1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico (1), idoneo a indicare il vincolo imposto a fini di giustizia.
2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria. (2)

3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione.
3-bis. L'autorità giudiziaria procede, altresì, anche su richiesta dell'organo accertatore alla distruzione delle merci di cui sono comunque vietati la fabbricazione, il possesso, la detenzione o la commercializzazione quando le stesse sono di difficile custodia, ovvero quando la custodia risulta particolarmente onerosa o pericolosa per la sicurezza, la salute o l'igiene pubblica ovvero quando, anche all'esito di accertamenti compiuti ai sensi dell'articolo 360, risulti evidente la violazione dei predetti divieti. L'autorità giudiziaria dispone il prelievo di uno o più campioni con l'osservanza delle formalità di cui all'articolo 364 e ordina la distruzione della merce residua. (3)
3-ter. Nei casi di sequestro nei procedimenti a carico di ignoti, la polizia giudiziaria, decorso il termine di tre mesi dalla data di effettuazione del sequestro, può procedere alla distruzione delle merci contraffatte sequestrate, previa comunicazione all'autorità giudiziaria. La distruzione può avvenire dopo 15 giorni dalla comunicazione salva diversa decisione dell'autorità giudiziaria. E' fatta salva la facoltà di conservazione di campioni da utilizzare a fini giudiziari. (3)
(1) Parole inserite dall'art. 8, comma 8, lett. a) della L. 18 marzo 2008, n. 48
(2) Periodo inserito dall'art. 8, comma 8, lett. b) della L. 18 marzo 2008, n. 48.
(3) Comma inserito dall'art. 2, comma 1, lett. a) del D.L. 23 maggio 2008, n. 92

Art. 352. Perquisizioni.
1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.
1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorche protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi. (1)
2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'articolo 380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.
3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'articolo 251 quando il ritardo potrebbe pregiudicarne l'esito.
4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.
(1) Comma inserito dall'art. 9, comma 1, della L. 18 marzo 2008, n. 48.

Art. 353. Acquisizione di plichi o di corrispondenza.
1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.
2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata e l'accertamento del contenuto. (1)

3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, (2) per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione (3) di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.
(1) Le parole: "*e l'accertamento del contenuto*" sono state aggiunte dall'art. 9, comma 2, lett. a), della L. 18 marzo 2008, n. 48
(2) Le parole: "*lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica*" sono state aggiunte dall'art. 9, comma 2, lett. b) della L. 18 marzo 2008, n. 48
(3) Le parole: "*telegrafico, telematico o di telecomunicazione*" sono state aggiunte dall'art. 9, comma 2, lett. b) della L. 18 marzo 2008, n. 48

Art. 354. Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.
1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. (1) Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale. (2)
(1) Il periodo che recita: "*In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*" è stato inserito dall'art. 9, comma 3, della L. 18 marzo 2008, n. 48
(2) Il periodo che recita: "*Se gli accertamenti comportano il prelievo di materiale biologico, si osservano le disposizioni del comma 2-bis dell'articolo 349.*" è stato soppresso dall'art. 27 della L. 30 giugno 2009, n. 85

6.12 Latvia

Expedited preservation

Latvian Criminal procedure law, Section 191. "Storage of Data located in an Electronic Information System":

- a person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system.

- the duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days.

Partial disclosure

Criminal procedure law, Section 192 "Disclosure and Issue of Data Stored in an Electronic Information System":

(2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, based on a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law.

6.13 Lithuania

National laws and other legal acts of the Republic of Lithuania allowing for the Lithuanian police to apply expedited preservation of stored computer data in the Lithuania are as follows:

1. The **Law on the Electronic Communications** of the Republic of Lithuania, No. IX-2135, 15 April 2004 (Official Gazette, No. 69-2382, 2004) (hereinafter referred to as "the **LEC**").

The **LEC** regulates social relations pertaining to electronic communications services and networks, associated facilities and services, use of electronic communications resources as well as social relations pertaining to radio equipment, terminal equipment and electromagnetic compatibility.
Article 65 Paragraph 2 of the **LEC** provides that in order to ensure accessibility of data for the purposes of investigation, disclosure and persecution of serious and grave crimes specified in the Criminal Code of the Republic of Lithuania, providers of a public communications network and/or public electronic communications services must preserve and submit free of charge to the competent institutions, in accordance with the procedure established by the law, generated or processed data indicated in the Annex 1 "Categories of Data to be Stored" of the LEC (see below):

„Categories Of Data To Be Stored

1. Data necessary to trace and identify the source of a communication:
1.1. Data concerning fixed network telephony and mobile telephony: 1.1.1. the calling telephone number;
1.1.2. name, surname and address of the subscriber or registered user of electronic communications services;
1.2. Data concerning Internet access, Internet e-mail and Internet telephony:
1.2.1. the user ID(s) allocated;
1.2.2. the user ID and telephone number allocated to any communication entering the public telephone network;
1.2.3. the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

2. Data necessary to identify the destination of a communication:
2.1. Data concerning fixed network telephony and mobile telephony:
2.1.1. the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
2.1.2. the name(s) and address(es) of the subscriber(s) or registered user(s);
2.2. Data concerning Internet e-mail and Internet telephony:
2.2.1. the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

2.2.2. the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication.

3. Data necessary to identify the date, time and duration of communication:
3.1. Data concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
3.2. Data concerning Internet access, Internet e-mail and Internet telephony:
3.2.1. the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

3.2.2. the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

4. Data necessary to identify the type of communication:
4.1. Data concerning fixed network telephony and mobile telephony: the telephone service used;
4.2. Data concerning Internet e-mail and Internet telephony: the Internet service used.

5. Data necessary to identify users' communication equipment or what purports to be their equipment:
5.1. Data concerning fixed network telephony, the calling and called telephone numbers;
5.2. Data concerning mobile telephony:
5.2.1. the calling and called telephone numbers;
5.2.2. the International Mobile Subscriber Identity (IMSI) of the calling party;
5.2.3. the International Mobile Equipment Identity (IMEI) of the calling party;
5.2.4. the IMSI of the called party;
5.2.5. the IMEI of the called party;
5.2.6. in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;
5.3. concerning Internet access, Internet e-mail and Internet telephony:
5.3.1. the calling telephone number for dial-up access;
5.3.2. the digital subscriber line (DSL) or other end point of the originator of the communication.
6. data necessary to identify the location of mobile communication equipment:
6.1. the location label (Cell ID) at the start of the communication;
6.2. data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained."
The data listed in the 1 Annex above, according to Article 66 Paragraph 6 of the **LEC** shall be stored by the providers for 6 months from the date of the communication.
According to Article 66 Paragraph 8 of the **LEC**, providers of a public communications network and/or public electronic communications services must store data in accordance with the following principles:
"1) the data must be of the same quality and subject to the same security and protection as the network data;
2) the data shall be subject to appropriate technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss or alteration, unauthorized or unlawful storage, processing, use or disclosure;
3) the data shall be subject to appropriate technical and organizational measures to ensure that access to them could get only by authorized personnel."

2. The **Law on Operational Activities** of the Republic of Lithuania, No IX-965, 20 June 2002 (Official Gazette No. 65-2633, 2002) (as last amended on 27 March 2012, No. XI-1941, Official Gazette No. 42-2043, entered into force since 7 April, 2012) (hereinafter referred to as "the **LOA**").

The LOA regulates the legal basis for operational activities, principles and tasks of operational activities, the rights and duties of entities of operational activities, the carrying out of operational actions and operational investigation, participation of persons in operational activities, the use and disclosure of operational intelligence as well as the financing, control, and scrutiny of these activities.

/.../

8. **Use of technical means in operational activities** shall mean the installation, operation or dismantling of technical means and other lawful actions related thereto. Technical means may be used in operational activities in accordance with the general and special procedure.

9. **Use of technical means in accordance with the special procedure** shall mean the use of technical means in operational activities authorised by a reasoned court ruling when monitoring or recording personal conversations, other communications or actions, where none of the participants in the conversation, other communications or actions is aware of such monitoring and it is implemented by restricting the individual's right to inviolability of private life in accordance with the procedure laid down by law. The monitoring of the content and recording of the personal information transmitted by electronic communications networks, even if one of the persons is aware of such control, shall be subject to a reasoned court ruling, with the exception of the cases when a person requests or consents to such monitoring or recording without making use of the services and equipment of the economic entities providing the electronic communications networks and/or services.

/.../

24. **Operational investigation** shall mean an organisational tactical form of operational activities covering operational actions, including the actions requiring a reasoned court ruling or a prosecutor's authorisation. In carrying out an operational investigation, entities of operational activities may process operational investigation files."

Article 7 Paragraph 4 of the **LOA** provides rights of entities of operational activities:

"4. Entities of operational activities shall, on the grounds for an operational investigation provided for in Article 9 of this Law and upon obtaining the authorisation specified in Articles 10, 11, 12 or 13 of this Law, have the right:

1) to covertly monitor postal items, document items, money orders and documents thereof, obtain information on the economic, financial operations of a natural or legal person and on the use of financial instruments and/or means of payment;

2) to use technical means and obtain information from the economic entities providing electronic communications networks and/or services in accordance with the special procedure;

3) in accordance with the procedure laid down by the Government upon co-ordination with the Bank of Lithuania, to obtain information from the Bank of Lithuania; to obtain information from commercial banks, other credit and financial institutions, also from other legal persons – in accordance with the procedure laid down by the Government;

4) to covertly enter residential and non-residential premises and vehicles and to inspect them, to temporarily seize and inspect documents, seize samples of substances, raw materials and production as well as other objects for investigation without disclosing the fact of seizure thereof;

5) to use the mode of conduct imitating a criminal act;

6) to carry out controlled delivery."

Article 9. Grounds for an Operational Investigation

An operational investigation shall be conducted, when:

1) characteristics of a criminal act have not been established, but information is available about a **grave** or **serious crime** being planned, being committed or having been committed or **less serious** crimes provided for in Article 131, paragraph 2 of Article 145, paragraphs 2 and 3 of Article 146, paragraph 2 of Article 151, Article 162, paragraph 2 of Article 178, paragraph 1 of Article 180, paragraph 1 of Article 181, paragraph 2 of Article 187, paragraph 2 of Article 189, paragraph 1 of Article 189_1, paragraph 2 of Article 198, paragraph 1 of Article 213, Articles 214 and 215, paragraph 1 of Article 225, paragraphs 1 and 2 of Article 226, paragraphs 1 and 2 of Article 227, paragraph 1 of

Article 228, Article 228$_1$, Article 240, paragraph 1 of Article 253, paragraph 1 of Article 256, paragraphs 2 and 3 of Article 300, paragraph 2 of Article 301, paragraph 2 of Article 302 and paragraphs 1 and 2 of Article 307 of the 103

Criminal Code of the Republic of Lithuania or about a person planning, committing or having committed a crime;
2) information is available about the activities of the special services of other states;
3) the suspect, the accused or the convicted person goes into hiding;
4) a person is reported missing;
5) protection of persons against criminal influence is being implemented;
6) protection of state secrets is being implemented;
7) information is available about the acts positing a threat to the constitutional system of the State, independence and economic security thereof, ensuring of the defence power of the State or other interests of importance to national security."

Article 10. Covert Monitoring of Postal Items, Document Items, Money Orders and Documents Thereof, Use of Economic, Financial Operations of a Natural or Legal Person, Financial Instruments and/or Means of Payment, Use of Technical Means in Accordance with the Special Procedure and Obtaining of Information from the Economic Entities Providing Electronic Communications Networks and/or Services, from the Bank of Lithuania, Commercial Banks, Other Credit and Financial Institutions, Also from Other Legal Persons

.....

3. The **Criminal Code** of the Republic of Lithuania, approved by the Law of the Republic of Lithuania No. VIII-1968, 26 September, 2000 (Official Gazette, No. 89-2741, No. 46, 2000) (as last amended by the Law No. XI-1861, 22 December, 2011, Official Gazette, No. 5-138, 2012, entered into force since 7 January, 2012) (hereinafter referred to as "the **CC**").

4. The **Code of the Criminal Procedure** of the Republic of Lithuania, approved by the Law of the Republic of Lithuania No. IX-785, 14 March, 2002 (Official Gazette, No. 37-1341, No. 46, 2002) (as last amended by the Law No. XI-1478, 21 June, 2011, Official Gazette, No. 81-3965, 2011, entered into force since 5 July, 2011) (hereinafter referred to as "the **CCP**").

The **CCP** regulates social relations pertaining to pre-trial investigations of criminal acts as well as proceedings in the criminal courts.

Article 154 of the **CCP** provides coercive investigative measure – the seizure of items, which are presumed to be evidences in the court:

"Article 147. Seizure

1. When it is necessary to obtain items or documents important for investigation of a criminal act and location or possessor thereof is known a pre-trial investigation officer or prosecutor may implement seizure. Seizure is imposed by a grounded ruling of a pre-trial investigation judge. In cases of emergency seizure can be implemented by a decision of a pre-trial investigation officer or prosecutor however, in such a case approval of a pre-trial investigation judge in respect of the implemented seizure shall be acquired within three days from the day of actual seizure. Upon failure to acquire approval of a pre-trial investigation judge within said term all the seized items and documents shall be returned to the persons from whom they were seized and the results of the seizure may not be used as evidence of guilt of the suspect or accused person.
2. Persons possessing items or documents to be seized shall not obstruct the officers implementing the seizure. Persons failing to comply with his duty may be fined further to the article 163 of this Code.

3. During seizure the persons specified in the part 4 article 145 of this Code shall be present.
4. If persons possessing the items or documents that must be seized fail to surrender them, the items or documents may be seized with the use of force." 104

Article 154 of the **CCP** provides coercive investigative measures for real time-control of the content, when pre-trial investigation is started:

"Article 154. Control, Recording and Accumulation of Information Transmitted through Electronic Communications Networks
1. Where there is an order of the judge of pre-trial investigation taken on the grounds of a prosecutor's request, a pre-trial investigation officer may wiretap conversations, transmitted through electronic communications networks, make records, control any other information transmitted through electronic communications networks and make records as well as accumulate if there are grounds to believe that in this way information may be obtained about a **grave crime** or **serious crime** or **less serious crime** either in preparation, in progress or already committed or about **minor crimes** foreseen in Article 170, Article 198(2) Paragraph 1, of the Criminal Code of the Republic of Lithuania, or if there is a danger that violence, coercion or other illegal actions may be used against a victim, witness or other parties to the proceedings or their relatives.
2. The order of the judge of a pre-trial investigation or the decision of a prosecutor to impose wiretapping conversations, transmitting through electronic communications networks, making records, controlling any other information transmitted through electronic communications networks and making records as well as accumulating must specify the following information…
Article 155 of the **CCP** provides investigative measure for collecting any kind of information during pre-trial investigation upon a request of the prosecutor or pre-trial investigation officer:

Article 155. Right of a Prosecutor to Get Familiarised with the Information
1. Having passed a decision and acquired approval of a pre-trial investigation judge a prosecutor has the right to visit any national or municipal, public or private institution, enterprise, or organisation and request to be allowed to get familiarized with the necessary documents or other information, make records or copies of the documents and information, or acquire information in written if this is necessary for investigation of a criminal act.
2. Pursuant to article 163 of this Code a fine can be imposed upon persons refusing to provide information or documents requested by the prosecutor.
3. A prosecutor may use the information acquired in the procedure specified in part 1 of this article only for the purpose of investigation of the criminal act. A prosecutor shall immediately destroy information not necessary for investigation of the criminal act.
4. A pre-trial investigation officer can be commissioned by a prosecutor to get familiarized with the information in the procedure defined by this article.
5. Laws of the Republic of Lithuania can establish limitations on the right of a prosecutor to get familiarized with information."

6.14 Republic of Moldova

Law on preventing and combating cybercrime (No. 20-XVI of 03.02.2009) - The Official Gazette No.11-12/17 of 26.01.2010

Article 7. Obligations of service providers

(1) Service providers are obliged:
a) to keep records of service users;
b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and

distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes;
c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation;
d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user;
e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system;
f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted
g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days.
(2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.
Law on preventing and combating cybercrime (No. 20-XVI of 03.02.2009) - The Official Gazette No.11-12/17 of 26.01.2010

Article 10. Requests of competent foreign authorities

(1) Within international cooperation, the competent foreign authority may request that the competent authority from the Republic of Moldova immediately preserve computer data or web traffic data existing in a computer system on the territory of the Republic of Moldova, regarding which the competent foreign authority will submit a well-founded request of international legal assistance in criminal matters.
(2) The request of immediate preservation described in paragraph (1) includes:
a) the name of the authority requesting the preservation;
b) the summary presentation of facts which form the object of prosecution and their legal ratiocination;
c) the computer data which are required to be preserved;
d) any available information necessary for the identification of the computer data owner and the localization of the computer system;
e) the utility of computer data, the necessity of their preservation;
f) the competent foreign authority's intention to submit a request of international legal assistance in criminal matters.
(3) The period of conservation of data recorded in par. (1) shall be not less than 60 calendar days and shall be valid until the competent national authorities decide upon the request of international legal assistance in criminal matters.
(4) Transmission of computer data shall be made only after the acceptance of the request of international legal assistance in criminal matters.

6.15 Norway

Preservation

Criminal Procedure Act section 215a:

”The prosecuting authority may as part of an investigation make an order concerning the securing of electronically stored data deemed to be significant as evidence.
An order concerning the securing of data in a communication that is in the possession of a provider of access to an electronic communications network or electronic communication service may only be made if the conditions in the first paragraph are fulfilled and there is reason to believe that a criminal act has been committed. The person who is entitled to dispose of the data covered by a security order shall be informed of the order. A suspect shall be informed as soon as the data has been secured and he as been given the status of a suspect. Otherwise information shall be given as soon as the data have been secured.
The security order shall apply for a specific period that must not be longer that necessary and not exceed 90 days at a time. If the security order is made at the request of a foreign State, it shall apply for at least 60 days. Sections 197, third paragraph, 208, first and third paragraphs, and 216 I shall apply correspondingly. The person who is subject to the order shall on application surrender the traffic data necessary for tracing where the data covered by the security order came from and where they may possibly be sent.”

Partial disclosure

For partial disclosure of traffic data, the Norwegian Post and Telecommunications Authority must exempt from the general duty of confidentiality, cf. the Electronic Communication Act Section 2-9 and the Criminal Procedure Act Section 118, first subsection:
”The court may not without the Ministry’s consent receive any evidence that the witness cannot give without breaching a statutory duty of secrecy that he has as a consequence of service or work for a family counseling office, a postal agency, a provider of access to an electronic communication network or electronic communication service, electronic communication electrician or the State Airport Company (Avinor). Consent may only be denied if the revelation may be detrimental to the State or public interest or have unfair results for the person who is entitled to the preservation of secrecy.
After giving due consideration to the duty of secrecy, on one hand, and to the clarification of the case, on the other, the court may by order decide that the evidence shall be given even though consent has been denied, or that evidence shall not be received even though the Ministry has consented. Before making such a deciscion, the court shall give the Ministry an opportunity to give an account of the reasons for its point of view. This account shall not be communicated to the parties.

The provision in section 117, second paragraph, shall apply correspondingly.”

”The Ministry” mentioned above, is in this case the Post and Telecommunication Authority.

6.16 Portugal

Law no. 109/2009 on Cybercrime of 15 September 2009:

Expedited preservation

Article 12
Expedited preservation of data
1 – If, during the proceedings, when gathering evidence in order to ascertain the truth, it is required to obtain specified computer data stored on a computer system, including traffic data, which might be lost, changed or no longer available, the competent judicial authority orders the person who has the control or availability of such data, including the service provider, to preserve the data in question.
2 - The preservation can also be ordered by the criminal police force, authorized by the judicial authority or even not in emergency or danger in delay but, in this case, notice must be given immediately to the judicial authority, by the report described under Article 253 of the Code of Criminal Procedure.
3 - A preservation order describes, under penalty of nullity:
a) the nature of the data;
b) the origin and destination, if known, and

c) the period of time covered by the preservation order, up to three months.
4 - In compliance with the preservation order addressed to it, whoever has availability or control over such data, including the service provider, preserves immediately the data concerned, protecting and maintaining their integrity for the appointed period of time, in view to allow the competent judicial authority to effectively obtain that information, and remains obliged to ensure the confidentiality of the implementation of these procedures.
5 - The competent judicial authority may order the renewal of the measure for periods of time according to the limit specified in c) of paragraph 3, providing all the requirements, up to a maximum of one year.

Partial disclosure

Article 13
Expedited disclosure of traffic data
In order to ensure the preservation of traffic data from a particular communication, regardless of the number of service providers participating in it, the service provider to whom the preservation has been ordered under the preceding article, discloses to the judicial authority or criminal police force, once known, other service providers through which this communication was carried out in order to identify all service providers used by that communication.

International preservation requests

Article 22
Preservation and expedited disclosure of computer data within international cooperation
1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data.
2 - The request specifies:
a) the authority requesting the preservation;

b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto;
c) the computer data to be retained and its relation to the offense;
d) all the available information to identify the person responsible for the data or the location of the computer system;
e) the necessity of the measure of preservation, and
f) The intention to submit a request for assistance for search, seizure and disclosure of the data.
3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them.
4 - Preservation can also be ordered by Polícia Judiciária, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article.
5 - A preservation order specifies, on penalty of nullity:
a) the nature of the data;
b) if known, the source and their destination, and
c) the period of time during which that data must be preserved for up to three months.
6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity.
7 - The competent judicial authority, or Policia Judiciária with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year.

8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request.
9 - Data preserved under this Article may only be provided:
a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17;
b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13.
10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data.
11 – The provisions of paragraphs 1 and 2 shall apply, mutatis mutandis, to requests sent to other authorities by the Portuguese authorities.

Article 23 - Grounds for refusal
1 - A request for expedited preservation or disclosure of computer data is refused if:
a) the computer data in question refer to a political offense or a related offense according to Portuguese law;
b) it attempts against the sovereignty, security, ordre publique or other constitutionally defined interests of the Portuguese Republic;
c) the requesting State does not provide guarantees for the protection of personal data.
2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.

6.17 Romania

Expedited preservation and partial disclosure

ART.54 of Romania Law no 161/2003
(1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.
ART. 55 of Romanian Law 161/2003(in view of making copies that can serve as evidence);
(1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court

of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, traffic data
or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.
(2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.
(3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

International cooperation
Art.63-64 Law no.161/2003
ART.63 of Romania Law no 161/2003
(1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal 110

matters.
(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation

b) a brief presentation of facts that are subject to the criminal investigation and their legal background;
c) computer data required to be preserved;
d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;
e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;
(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters.
Art.64 of the Law no.161/2003
If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

6.16 Serbia
General provisions of article 85 paragraph 1, 146 paragraph 1 and 7, article 155, and 255 paragraph 2, can be applied.

ARTICLE 85
(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.
….
amendment 11/9/2009 "Official gazette of Republic Serbia 72/2009"

(4)Measures referred to par 1 of this article shall be reviewed every three months and can last up to nine months. Implementation of measures will be stopped as soon as the reasons for their application are ceased.

6.17 Slovakia

Code of Criminal Procedure

Section 90 of the Code of Criminal Procedure

Preservation and Disclosure of Computer Data

(1) If the preservation of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including traffic data that is stored through a computer system, the presiding judge and, before the initiation of the criminal prosecution or in the preliminary hearing, the public prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to
a) store such data and maintain the integrity thereof,
b) allow the production or retention of a copy of such data,
c) render access to such data impossible,
d) remove such data from the computer system,
e) release such data for the purposes of the criminal proceedings.
(2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data storage shall be performed must be determined. This period may be up to 90 days, and if its re-storage is necessary, a new order must be issued.
(3) If the storage of the computer data, including the traffic data for the purpose of the criminal proceedings, is no longer necessary, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, shall issue an order for the revocation of the storage of such data without undue delay.
(4) The order under Subsection 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order.
(5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1.

Section 116 of the Code of Criminal Procedure

(1) In criminal proceedings for an intentional criminal offence, an order for the determination and notification of data on the performed telecommunications operation, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued.
(2) The warrant for the establishment and notification of data on the performed telecommunication operations shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing upon the petition of the public prosecutor, the judge for preliminary hearing, in writing which must be justified by its merits; the warrant shall be served to the persons referred to in Subsection 3. 112

Letters Rogatory of Foreign Authorities

Section 537
Method and Form of Letters Rogatory Processing

(1) The Slovak authorities shall perform the legal assistance requested by the foreign authorities in the manner regulated by this Act or an international treaty. If legal assistance is provided under an international treaty in a manner which is not governed by this Act, the competent public prosecutor shall decide in what manner the legal assistance should be performed.
(2) The requested legal assistance may be performed upon the request of a foreign authority under a legal regulation of the requesting State, if the requested procedure is not contrary to the interests protected by the provisions of Section 481.
(3) For the performance of letters rogatory under Section 539 Subsection 1, it is requested that the act, which the letters rogatory concern, is a criminal offence not only under the legal system of the requesting State, but also the legal system of the Slovak Republic.
Section 538
Jurisdiction for the Processing of Letters Rogatory
(1) The letters rogatory of a foreign authority for legal assistance shall be served to the Ministry of Justice.
(2) To ensure the processing of a letter rogatory from a foreign authority for legal assistance, the district prosecution, under which jurisdiction the requested act of legal assistance is to be performed, is competent. If the local jurisdiction is given to several public prosecutions, the Ministry of Justice shall send the letters rogatory to the Attorney General's Office for a decision as to which of the public prosecutions shall provide its processing.
(3) If a foreign authority requests the performance of an interrogation or another act of legal assistance by the court due to the application of the act in the criminal proceedings in the requesting State, the public prosecutor shall submit the letters rogatory of a foreign authority to this extent to the District Court under which jurisdiction the act of legal assistance is to be performed, for processing. If the subject of the letters rogatory is solely an act which is to be performed by the court, the Ministry of Justice shall serve the request directly to the competent court.

Section 539
Permission of an Act of Legal Assistance for the Courts

(1) If the order of the court under this Act is necessary for the performance of evidence requested by a foreign authority, the court shall issue an order upon the petition of the public prosecutor providing the processing of the letters rogatory.
(2) If the act of legal assistance is to be performed under a foreign regulation, the court shall decide, upon the petition of the public prosecutor, whether the procedure under the foreign regulation is not contrary to the interests protected by the provisions of Section 481. If they do not find such conflict, the act shall be permitted and they shall simultaneously decide on the manner of its performance. The public prosecutor may file a complaint against the decision of the court, which has a suspensive effect. The decision of the court on the conflict of the procedure under a foreign regulation shall not be required if it is a serving of documents or instruction of the person under a foreign regulation.
(3) The District Court under which jurisdiction the act of legal assistance is to be performed is competent to make a decision under Subsection 1 and 2.

6.18 Slovenia

Criminal Procedure Law

Article 148

(1) If there are grounds for suspicion that a crime was committed for which the offender is prosecuted ex officio, the police must take steps necessary to trace the offender, that the offender or participant does not hide or flee, to detect and protect the traces of a criminal offense and objects which may be used as evidence and to collect all information that could be useful for the successful conduct of criminal proceedings.

Article 149b

(1) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the state prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.
(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an adducement of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.
(3) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator of the electronic communications network furnish it with this information, at its written request and even without the consent of the individual to whom the information refers.
(4) The operator of electronic communications networks may not disclose to its clients or a third party the fact that it has given certain information to an investigating judge (first paragraph of this article) or the police (preceding paragraph), or that it intends to do so.".

Article 150

(1) If there are well-founded grounds for suspecting that a particular person has committed, is committing or is preparing or organising the committing of any of the criminal offences listed in the second paragraph of this Article, and if there exists a well-founded suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not permit the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person:
1) the monitoring of electronic communications using listening and recording devices and the control and protection of evidence on all forms of communication transmitted over the electronic communications network;
2) control of letters and other parcels;
3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities;

4) wire-tapping and recording of conversations with the permission of at least one person participating in the conversation;

Article 164
(1) The police may even prior to the initiation seize items at 220th of this Act, if it would be dangerous to delay, and the conditions of the 218th of this Act to make home and personal investigation.

Article 220 (seizure of items)
(1) Items which must be take under criminal or may be evidence in criminal proceedings shall be seized and deposited with the court or otherwise protect their storage.
(2) A person who has such items tmust delivered them at the request of the court. If he does not deliver the items, they can to be punished by a fine specified in the first paragraph of Article 78 of this Act, if he still don't want to do, he can be put in prison. Prison lasts until the surrender pf items or until the end of criminal proceedings, but more than one month.
(4) Police officers may seize items mentioned in the first paragraph of this Article, when act in connection with 148t and 164 Article of this Act or when they issuing the court order.

Article 223
(1) The investigating judge may order that the postal, telegraph and other transport organizations and detained against acknowledgment of receipt handed him a letter, telegraph and other items, which are addressed to the defendant or that he sends, if the circumstances, which may cause reasonably be expected to demonstrate in the shipment process.

6.19 "The former Yugoslav Republic of Macedonia"

Criminal Procedure Code (old code)

Temporary securing and seizing of objects or property

Article 203

(1) Objects which according to the Criminal Code are to be seized or may serve as evidence in the criminal procedure, shall be temporarily seized and handed to the court to guard or in another manner secure their guarding.
(2) Whosoever holds such objects shall be obliged to hand them over to the court on its request. The person who refuses to hand over the objects may be punished with a fine determined in Article 74, paragraph 1 of this Code.
(3) The council (Article 22, paragraph 6) shall decide upon an appeal against the determination that imposes a fine. The appeal against the determination shall not withhold the enforcement of the determination.
(4) The authorized officials of the Ministry of Interior can seize the objects listed in paragraph 1 of this Article when they act according to Articles 142 and 147 of this Code or when they execute a court order.
(5) Upon the seizing of the objects the location where they are found shall be notified and described, and if necessary confirmation of their identity shall be provided in another manner. A proof shall be issued for the seized objects.
(6) The confiscated narcotic drugs, psychotropic substances, precursors and other objects prohibited or limited for trade, which are not kept as samples for expertise, by the decision of the competent court, can be destroyed even before the verdict becomes legally valid.

Article 203-a

(1)The investigating judge or the council can, with a determination, stipulate temporary securing of property and means related to the crime. The property and means being subject to securing shall be under court's

supervision. Temporary securing of property or objects refers to temporary freezing, confiscation, holding funds, bank accounts and financial transaction or incomes from the crime.
(2)Apart from the objects referred to in Article 203 of this Code, the court can adopt a decision for freezing the means, accounts and funds being suspected to be income from the crime.
(3)The measures for temporary securing of objects, property or means can last until the end of the procedure.
(4)The temporary freezing of accounts can last until the end of the procedure, and its justification shall be re-examined ex officio every two months.
(5)The securing of the immovables shall be done with encumbering a mortgage.
(6)The confiscation of the monetary funds shall be made with an order and they shall be kept in a safety deposit box, or be deposited on a special account without the right to their disposal.
(7)The determination on freezing the financial transaction or bank account shall be submitted to the bank by the court or by other financial institution.
(8)No one can call upon the bank secrecy in order to avoid the enforcement of the court's determination for temporary freezing, confiscation or holding of the funds deposited in the bank.

Article 203-b

A determination for temporary securing of objects or property can be adopted by a court on a request from a foreign state, in the cases anticipated in the international agreements in accordance with the Constitution of the Republic of Macedonia.

Article 203-c

(1)With the determination referred to in Article 203-a of this Code the following cannot be seized: - the records or other documents of the state bodies which if published could violate the keeping of an official, state or military secrecy, until the competent body decides otherwise; - the written documents addressed from the defendant to the attorney and the persons referred to in Article 219, paragraph (1) of this Code, unless the defendant hands them in voluntarily; - technical recordings in possession of the persons referred to in Article 219, paragraph (1) of this Code, made by those persons for facts being released from their duty to testify thereof; - recordings, excerpts from the register and similar documents in possession of the persons referred to in Article 219, paragraph (1) of this Code, made by them for facts for which they acknowledged from the defendant during their work and
- recordings for facts made by journalists and their editors in mass media from the source of announcement and the information they have acquired during their work and which were used during the editing process of the mass media, which are in their possession or in the redaction where they are employed.
(2)The prohibition of paragraph (1) of this Article shall not apply:
- towards the attorney or the person released from the obligation to testify according to Article 219, paragraph (1) of this Code, if there is a grounded suspicion that they have helped the defendant in committing the crime, or they provided him assistance after the crime was committed or have acted as conceivers or - if it is a matter of objects which must be seized according to the Criminal Code.
(3)A prohibition for temporary seizing of documents, objects and technical recordings as referred to in paragraph (1) of this Article, shall not apply to crimes regarding damage against children and juveniles. The information kept in devices for automatic i.e. electronic processing of the data and media have to be handed in to the bodies in the criminal procedure in a readable and comprehensible form upon a request of the investigating judge, the council or the sole judge.

Article 203-d

(1)The measures for temporary securing and seizing of objects or property shall be stipulated by a court determination, meaning the investigating judge during the investigation and after initiation of an indictment, the judicial council i.e. a sole judge.
(2)The criminal council, referred to in Article 22 paragraph (6) of this Code, shall decide upon the appeal against the determination of the investigating judge, and the immediate court of higher instance shall decide upon the determination of the trying judge, i.e. of the council.
(3)The objects seized against this Article cannot be used as evidence in the procedure.

Article 204

(1)The state bodies can prohibit showing or issuing of their records or other documents if they consider the issuing of their contents to be harmful to the interests of the state. If the showing or issuing records or other documents is not allowed, the council (Article 22, paragraph 6) shall adopt a final decision.
(2) Legal entities can request the data referring to their work not to be issued.

Article 205

(1) If temporary seizing of records, which may serve as evidence, is performed, such evidence shall be registered. If it is not possible, the records shall be wrapped in a case and shall be sealed. The holder of the records can put his seal on the case.

(2) The person wherefrom the records are seized shall be invited to attend the opening of the case. If he does not reply on the invitation or is absent, the case shall be opened the records shall be inspected and listed in his absence.
(3) During the inspection of the records it must be secured that unauthorized persons would not have access to their contents.

Article 206

(1) The investigating judge can order the legal entities in the field of post, telegraph and other traffic, to keep and, with a confirmation of the receipt, to give to the investigating judge the letters, telegrams and other items addressed to the defendant or sent by the defendant, if there are circumstances according to which it could be expected that these items may serve as evidence in the procedure.
(2) The letters and other parcels shall be opened by the investigating judge in presence of two witnesses. The opening shall be conducted cautiously, in order not to damage the seals, and the case and address shall be kept. Minutes shall be composed for the opening.
(3) If the interests of the procedure allow, the contents of the item can be announced fully or partially to the defendant i.e. the person to whom it is addressed and it may also be handed over to him. If the defendant is absent the item shall be announced or handed over to one of his relatives, and if he has none, it shall be handed to the sender if that does not confront the interests of the procedure.

New Criminal Procedure Law (enters into force in November 2012)

Article 184

Search of a computer system and computer data

(1) Upon request by the person who executes the warrant, the person who uses the computer or has access to it or to another device or data carrier, shall be obliged to provide access to them and give all necessary information required for unobstructed fulfillment of the goals of the search.

(2) Upon request by the person who executes the warrant, the person who uses the computer or has access to it or to another device or data carrier, shall be obliged to immediately take all necessary measures required to prevent the destruction or change of the data.
(3) Any person who uses the computer or has access to it or to another device or data carrier, who fails to proceed pursuant to paragraphs 1 and 2 of this Article, without any justified reasons, shall be punished by the preliminary procedure judge, in accordance with the provisions of Article 88, paragraph 1 of this Law.

6.20 Ukraine

Extract of the new Criminal Procedure Code adopted in April 2012 and entered into force on 19 November 2012:

§ 2. Interference in private communication

Article 258. General provisions related to interference in private communication
1. Nobody may be subjected to interference in private communication without investigating judge's ruling.
2. Public prosecutor, investigator upon approval of public prosecutor shall be required to apply to investigating judge for permission to interfere in private communication as prescribed in Articles 246, 248-250 of the present Code, if any investigative (detective) action implies such interference.
Whenever investigating judge passes the ruling to deny interference in private communication, public prosecutor, investigator may file a new request only with new information.
3. Communication is transmitting information in any way from one person to another directly or using any connection. Communication is considered to be private insofar as information is transmitted and stored under such physical or legal conditions where participants to the communication can expect that such information is protected from interference on the part of others.
4. Interference in private communication implies access to the contents of communication under conditions when participants to the communication can reasonably expect that their communication is private. The following shall be types of interference in private communication:
1) audio, video monitoring of an individual;
2) arrest, examination and seizure of correspondence;
3) collecting information from telecommunication networks;
4) collecting information from electronic information systems.
5. Interference in private communication of defense counsel, between clergyman and the suspect, accused, convict, acquitted shall be forbidden.

Article 259. Preservation of information
1. If public prosecutor intends to use as evidence, during trial, information or any fragment of information obtained as a result of interference in private communication, he shall be required to ensure preservation of all information or delegate preservation of all information to the investigator.

Article 260. Audio, video monitoring of an individual
1. Audio, video monitoring of an individual is a variety of interference in private communication conducted without the individual's knowledge on grounds of a ruling of investigating judge if there are sufficient grounds for the belief that this individual's conversations or other sounds, movements, actions related to his activity or place of stay, etc., can contain information of importance for pre-trial investigation.

Article 261. Arrest of correspondence
1. An individual's correspondence may be arrested without he being aware thereof in exceptional cases based on investigating judge's ruling.

2. Correspondence is arrested if, in the course of pre-trial investigation, there are sufficient grounds for the belief that mail and cable correspondence a certain individual sends to other individuals or is sent from other individuals to the individual concerned, can contain information on circumstances which have importance for pre-trial investigation or objects and documents which have essential importance for pre-trial investigation.
3. Arrest of correspondence entitles the investigator to inspect and seize arrested correspondence.
4. Correspondence referred to in the present Article shall include letters of all types, postal packets, parcels, postal containers, postal money orders, telegrams, and other material mediums for exchange of information among individuals.
5. After the time limit specified in court's ruling has expired, arrest of individual's correspondence is deemed to be revoked.

Article 262. Inspection and seizure of correspondence

1. Seized correspondence shall be inspected in the postal office, which was assigned control and seizure of this correspondence, with participation of this office's representative and, in case of need, of a specialist. In the presence of the said individuals, investigator decides on the opening of correspondence and inspects seized correspondence.
2. Should objects (inclusive of substances), documents be found in the correspondence that are important for a certain pre-trial investigation, investigator within the scope prescribed in the investigating judge's ruling, shall conduct seizure of the correspondence concerned or limit himself to making copies or taking samples of relevant messages. Copies are made or samples taken in view of protecting confidentiality of correspondence arrest. If necessary, the person who inspects mail and cable correspondence, may take a decision to put special marks on the detected objects and documents, equip them with technical control devices, replace objects and substances which endanger surrounding people or are prohibited from being in free circulation, with their safe analogues.
3. If objects or documents of importance for pre-trial investigation are not found in the correspondence, investigator shall give instruction to deliver the correspondence inspected to the addressee.
4. A record shall be drawn up of each occurrence of inspection, seizure or arrest of correspondence as prescribed in the present Code. The record should necessarily state what kind of messages have been inspected, what has been seized from the messages, and what should be delivered to the addressee or temporarily kept, and from what messages copies or samples have been made, and the conduct of other actions as provided for in part two of this Article.
5. Managers and employees of postal offices shall be required to facilitate conducting this covert investigative (detective) action and not to disclose the fact of conducting this covert investigative (detective) action or the information obtained.

Article 263. Collecting information from transport telecommunication networks

1. Collecting information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.
2. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment which can be used for interference in private communication.
3. Collecting information from transport telecommunication networks means the conducting using appropriate watch facility the surveillance, selection and recording information which is transmitted by an individual and have the importance for pre-trial investigation and also receiving, transformation and recording signals of differebt types which are transmitted by communication channels.

4. Collecting information from transport telecommunication networks is made by responsible units of the bodies of internal affairs and bodies of security. Managers and employees of telecommunication networks' operators shall be required to facilitate conducting the actions on collecting information from transport telecommunication networks, taking required measures in order not to disclose the fact of conducting such actions and the information obtained, and to preserve it unchanged.

Article 264. Collecting information from electronic information systems

1. Search, detection, and recording information stored in an electronic information system or any part thereof, access to the information system or any part thereof, as well as obtainment of such information without knowledge of its owner, possessor or keeper may be made based on the ruling rendered by the investigating judge, if there is information that such information system or any part thereof contains information of importance for a specific pre-trial investigation.
2. Obtainment of information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection, shall not require permission of investigating judge.
3. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics of the electronic information system which can be used for interference in private communication.

Article 265. Recording and preserving information obtained from communication channels through the use of technological devices and as a result of collecting information from electronic information systems

1. Contents of information which is transmitted by persons via the transport telecommunication networks shall be stated in the record of conducting of the said covert investigative (detective) actions. If such information is found to contain knowledge of importance for a specific pre-trial investigation, the record should reproduce its respective part, and then public prosecutor shall take measures to preserve information obtained by monitoring.
2. Contents of information obtained as a result of monitoring an information system or any part thereof, shall be recorded on the appropriate medium by the individual who has been responsible for monitoring and who is required to ensure processing, preserving, and transmitting the information.

Article 266. Examination of information obtained through the use of technological devices

1. Information obtained through the use of technological devices shall be examined, if necessary, with participation of a specialist. Investigator analyzes contents of the information obtained and draws up a record thereof. In case of detection of information of importance for pre-trial investigation and trial, the record should reproduce the appropriate part of information and then public prosecutor takes measures to preserve information obtained.
2. Technological devices which have been used during the conduct of the said covert investigative (detective) actions, as well as original mediums for received information shall be preserved till the judgment takes legal effect.
3. Mediums and technological devices which helped obtain information may be the subject of examination by appropriate specialists or experts as prescribed in the present Code.

6.21 United Kingdom

Police and Criminal Evidence Act 1984

http://www.legislation.gov.uk/ukpga/1984/60/schedule/1

http://www.homeoffice.gov.uk/publications/police/operational-policing/pace-codes/pace-code-b-2011?view=Binary

Regulation of Investigatory Powers Act (2000)
http://www.legislation.gov.uk/ukpga/1984/60/schedule/1_121

Acquisition and Disclosure of Communications Data Code of Practice [2007]

Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary

This Code of Practice provides for access to retained data.

6.22 USA

The U.S. Federal Criminal Code, found at Title 18 of the U.S. Code, includes a provision for data preservation, specifically at U.S. Code, Title 18, Section 2703(f).

The text:

18 U.S.C. § 2703. Required disclosure of customer communications or records.
...
(f) Requirement To Preserve Evidence.—
(1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
(2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.
Law enforcement officials obtain partial disclosure of traffic data by issuing a subpoena, as set forth at U.S. Code, Title 18, Section § 2703(c), as follows. Underlined items include the partial disclosure of traffic data.

18 U.S.C. § 2703. Required disclosure of customer communications or records.
...
(c) Records Concerning Electronic Communication Service or Remote Computing Service.
...
(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—
(A)name;
(B)address;
(C)local and long distance telephone connection records, or records of session times and durations;
(D)length of service (including start date) and types of service utilized;
(E)telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F)means and source of payment for such service (including any credit card or bank account number),
of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena... .

7 Appendix 2: Extracts of the Budapest Convention on Cybercrime and explanatory report

7.1 Article 16 –Conservation rapide de données informatiques stockées

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

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

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

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

Rapport explicatif:

Titre 2 – Conservation rapide de données stockées

149. Les mesures mentionnées dans les articles 16 et 17 s'appliquent aux données stockées qui ont déjà été collectées et archivées par les détenteurs de données, tels que les fournisseurs de services. Elles ne s'appliquent pas à la collecte en temps réel et à la conservation de futures données relatives au trafic ni à l'accès en temps réel au contenu des communications. Ces questions sont traitées au Titre 5.
150. Les mesures décrites dans ces articles ne sont applicables que lorsque les données informatiques existent déjà et sont en cours de stockage. Il peut exister bien des raisons pour lesquelles les données informatiques présentant un intérêt pour les enquêtes pénales n'existent pas ou ne sont plus stockées. Ainsi, par exemple, on peut n'avoir ni collecté ni conservé des données exactes ou, si on en a collecté, on ne les a pas conservées. Les lois régissant la protection des données peuvent avoir imposé la destruction de données importantes avant que qui que ce soit ne réalise leur importance pour la procédure pénale. Parfois, il n'existe pas de motif commercial pour collecter et conserver des données, comme dans le cas où les clients paient un tarif forfaitaire pour des services ou que les services sont gratuits. Les articles 16 et 17 n'abordent pas ces problèmes.
151. Il importe d'établir une distinction entre la "conservation des données" et l'"archivage des données". Les deux expressions ont des sens voisins dans le langage courant, mais différents en informatique. Conserver des données, c'est garder des données qui existent déjà sous une forme stockée et en les protégeant contre tout ce qui pourrait en altérer ou en dégrader la qualité ou l'état actuel. Archiver des données, c'est garder en sa possession pour l'avenir des données qui sont en cours de production. L'archivage des données implique l'accumulation des données dans le présent et la garde ou la possession de ces données en prévision d'une période future. L'archivage des données

est le processus de stockage des données. En revanche, la conservation des données est l'activité qui garantit leur sécurité et leur sûreté.

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

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

154. Dans certains États, la loi requiert que certains types de données, telles que les données personnelles, en la possession de certaines catégories de détenteurs ne soient pas archivées, mais effacées lorsque leur archivage ne répond plus à une fin commerciale. Dans l'Union européenne, le principe général est mis en pratique par la Directive 95/46/EC et, dans le contexte particulier du secteur des télécommunications, par la Directive 97/66/EC. Ces directives instaurent l'obligation d'effacer les données dès que leur stockage n'est plus nécessaire. Toutefois, les États membres peuvent adopter une législation prévoyant des dérogations lorsqu'elles sont nécessaires pour prévenir la commission d'infractions pénales, instruire les infractions ou poursuivre leurs auteurs. Ces directives n'empêchent pas les États membres de l'Union européenne d'instaurer des pouvoirs et procédures en droit interne pour conserver des données spécifiées aux fins d'enquêtes spécifiques.

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

d'autres infractions ont été commises, par exemple des cas de trafic de stupéfiants ou d'escroquerie. L'identification de la source ou de la destination de ces communications antérieures peut aider à établir l'identité des auteurs de ces infractions. Pour déterminer la source ou la destination de ces communications, il faut disposer de données relatives au trafic concernant ces communications antérieures (pour d'autres explications sur l'importance des données relatives au trafic, se reporter à l'article 17 ci-dessous). Troisièmement, lorsque ces communications présentent un contenu illicite ou la preuve d'agissements criminels et que des copies de ces communications sont archivées par les fournisseurs de services (de courrier électronique, par exemple), la conservation de ces communications est importante afin de ne pas perdre des éléments de preuve essentiels. L'obtention de copies de ces communications antérieures (par exemple de courriers stockés qui ont été envoyés ou reçus) peut révéler que des infractions ont été commises.

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

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

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

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

159. La 'conservation' exige que les données qui existent déjà et sont stockées soient protégées contre tout ce qui risquerait d'en modifier ou dégrader la qualité ou l'état actuel. Elle exige que les données soient maintenues à l'abri de toute modification, de toute détérioration ou de tout effacement. La conservation n'implique pas nécessairement que les données soient 'gelées' (c'est-à-dire rendues inaccessibles) et que ces données ou des copies de ces données ne puissent pas être utilisées par des utilisateurs légitimes. La personne à laquelle est adressée l'injonction peut, en fonction des spécifications exactes de celle-ci, conserver l'accès aux données. L'article ne précise pas la manière dont les données doivent être conservées. Il appartient à chaque Partie d'établir les modalités appropriées de conservation et de déterminer si, dans certains cas, la conservation des données devrait également comporter le 'gel' de celles-ci.

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

161. Le pouvoir d'ordonner ou d'obtenir d'une autre manière la conservation rapide de données électroniques spécifiées s'applique à tout type de données informatiques stockées. Il peut s'agir de tout type de données qui est spécifié dans l'ordre de conserver, comme des dossiers commerciaux, médicaux ou personnels. Les Parties doivent instaurer ces mesures pour les appliquer "notamment lorsqu'il y a des raisons de penser que [les données] sont particulièrement susceptibles de perte ou de modification." Il peut se faire, par exemple, que les données ne soient archivées que pour une brève période. C'est le cas, par exemple, lorsqu'une entreprise a pour politique d'effacer les données au bout d'un certain temps ou que les données sont systématiquement effacées lorsque le support de stockage est utilisé pour enregistrer d'autres données. Le risque peut également tenir aux caractéristiques du gardien des données ou au fait que les données sont stockées d'une manière qui n'en garantit pas la protection. Toutefois, si le gardien n'était pas digne de confiance, il serait plus sûr de procéder à la conservation par perquisition et saisie plutôt que par une injonction à laquelle l'intéressé pourrait ne pas obtempérer. Le paragraphe 1 mentionne expressément les "données relatives au trafic" afin d'indiquer l'applicabilité particulière de ces dispositions à ce type de données, lesquelles, lorsqu'elles sont collectées et archivées par un fournisseur de services, ne sont généralement conservées que une brève période. Par ailleurs, la mention des "données relatives au trafic" établit un lien entre les mesures visées aux articles 16 et 17.

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

163. Le paragraphe 3 impose une obligation de confidentialité sur la mise en oeuvre des procédures de conservation au gardien des données ou à une autre personne à qui il est enjoint de conserver celles-ci pendant la durée prévue par son droit interne. Les Parties sont ainsi tenues d'instaurer des mesures de confidentialité concernant la conservation rapide de données stockées ainsi qu'une durée maximale de confidentialité. Cette mesure tient compte des besoins de la lutte contre la criminalité en faisant en sorte que le suspect faisant l'objet d'une enquête n'ait pas connaissance de celle-ci, ainsi que du droit des particuliers au respect de leur vie privée. Pour les services de lutte contre la criminalité, la conservation rapide des données s'inscrit dans le cadre des enquêtes préliminaires, période durant laquelle il peut être important de conserver le secret. La conservation est une mesure préliminaire adoptée en attendant que soient prises d'autres mesures juridiques visant à obtenir les données ou leur divulgation. La confidentialité s'impose pour éviter que d'autres personnes ne tentent de manipuler ou d'effacer les données. Pour la personne à laquelle l'injonction est adressée, la personne concernée ou d'autres personnes pouvant être mentionnées ou identifiées dans les données, la durée maximale de la mesure est bien spécifiée. La double obligation de garantir la sécurité des données et de s'assurer que le secret sur la mise en oeuvre de la mesure de conservation est gardé

contribue à défendre le droit à la vie privée de la personne concernée ou des autres personnes pouvant être mentionnées ou identifiées dans ces données.
164. En sus des limitations précitées, les pouvoirs et procédures mentionnés dans l'article 16 doivent être soumis aux conditions et sauvegardes prévues aux articles 14 et 15.

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

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

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

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

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

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

165. Cet article instaure des obligations spécifiques concernant la conservation des données relatives au trafic visées à l'Article 16 et prévoit la divulgation rapide de certaines données relatives au trafic aux fins d'identification des autres fournisseurs de services ayant participé à la transmission de communications spécifiées. Les "données relatives au trafic" sont définies à l'article premier.
166. L'obtention de données relatives au trafic stockées concernant des communications antérieures peut être indispensable pour déterminer la source ou la destination de ces communications, ce qui est essentiel pour identifier les personnes qui, par exemple, ont distribué de la pornographie enfantine, diffusé de fausses déclarations dans le cadre d'une manœuvre frauduleuse, propagé des virus informatiques, tenté d'accéder de façon illicite à des systèmes informatiques ou réussi à le faire, ou transmis à un système informatique des communications qui ont soit porté atteinte aux données du système, soit entravé le bon fonctionnement de celui-ci. Or, ces données ne sont souvent stockées que pour une courte durée, la législation protégeant le droit au respect de la vie privée pouvant interdire le stockage de longue durée de ces données quand ce ne sont pas les forces de marché qui le découragent. Il est donc important de mettre en oeuvre des mesures de conservation pour garantir l'intégrité de ces données (on se reportera à l'analyse de la question de la conservation ci-dessus).
167. Il arrive souvent que plusieurs fournisseurs de services participent à la transmission d'une communication. Chaque fournisseur peut posséder certaines données relatives au trafic concernant la transmission de la communication spécifiée, qui ont soit été produites et archivées par ce fournisseur à l'occasion du passage de la communication par son système, soit ont été fournies par d'autres fournisseurs. Il arrive que les données relatives au trafic, ou tout au moins certains types de données relatives au trafic, soient partagées entre les fournisseurs de services ayant participé à la transmission de la communication, à des fins commerciales, sécuritaires ou techniques. En pareil cas, l'un ou l'autre de ces fournisseurs peut posséder les données relatives au trafic essentielles pour déterminer la source ou la destination de la communication. Souvent, toutefois, aucun fournisseur ne possède à lui seul suffisamment de données relatives au trafic pour permettre de déterminer avec exactitude la

source ou la destination de la communication. Chacun possède certaines parties du puzzle et chacune de ces parties doit être examinée afin d'identifier la source ou la destination.

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

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

7.3 Article 29 – Conservation rapide de données informatiques stockées

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

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

a l'autorité qui demande la conservation;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique;

e la nécessité de la mesure de conservation; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

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

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

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

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

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

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

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

Rapport explicatif:

Conservation rapide de données informatiques stockées (article 29)

282. Cet article institue au niveau international un mécanisme équivalent à celui que prévoit l'article 16 au niveau national. Le paragraphe 1 de cet article autorise une Partie à demander, et le paragraphe 3 impose à chaque Partie de se donner les moyens juridiques d'obtenir, la conservation rapide de données stockées au moyen d'un système informatique sur le territoire de la Partie requise,

afin que les données ne soient pas modifiées, enlevées ou effacées pendant la période nécessaire à la préparation, à la transmission et à l'exécution d'une demande d'entraide aux fins d'obtention des données. La conservation est une mesure limitée de caractère provisoire destinée à intervenir de façon beaucoup plus rapide que l'exécution d'une requête d'entraide classique. Comme on l'a déjà indiqué, les données informatiques sont des plus volatiles. Il suffit de presser sur quelques touches ou d'utiliser des programmes automatiques pour les effacer, les modifier ou les déplacer, ou pour rendre impossible de remonter jusqu'à l'auteur de l'infraction constatée, voire pour détruire les preuves décisives de sa culpabilité. Certains types de données informatiques ne sont stockés que pour de brèves périodes avant d'être effacées. Il a donc été décidé qu'il fallait instituer un mécanisme qui garantirait la disponibilité de ces données pendant le déroulement du processus long et complexe de l'exécution d'une requête officielle d'entraide, qui peut s'étaler sur des semaines ou des mois.

283. Plus rapide que la méthode d'entraide habituelle, cette mesure est en même temps moins intrusive. Il n'est pas demandé aux responsables de l'entraide de la Partie requise d'obtenir la possession des données auprès de leur gardien. On juge préférable que la Partie requise s'assure que le gardien (qui est souvent un fournisseur de services ou une autre tierce partie) conserve (c'est-à-dire n'efface pas) les données en attendant que soit ordonnée leur remise ultérieure aux services chargés de l'application de la loi. Cette procédure a l'avantage d'être rapide et de respecter le droit de la personne concernée au respect de sa vie privée, car les données ne seront divulguées à un fonctionnaire quelconque ou examinées par celui-ci que lorsqu'il aura été satisfait aux critères applicables à la divulgation intégrale en conformité avec les accords d'entraide normaux. D'un autre côté, une Partie requise est autorisée à utiliser d'autres procédures pour garantir la conservation rapide des données, y compris la délivrance et l'exécution accélérées d'une injonction de produire ou d'un mandat de perquisition. L'élément primordial est de pouvoir engager un processus extrêmement rapide pour empêcher les données d'être perdues à jamais.

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

285. Le paragraphe 3 énonce le principe selon lequel la double incrimination n'est pas requise comme condition préalable à la conservation. D'une façon générale, l'application du principe de la double incrimination est contre-productive en matière de conservation. Tout d'abord, du point de vue de la pratique contemporaine de l'entraide, on constate une tendance à éliminer la règle de la double incrimination pour toute les mesures procédurales sauf les plus intrusives, telles que la perquisition et la saisie ou l'interception. Or, telle que l'ont conçue les auteurs de la Convention, la conservation n'est pas particulièrement intrusive dans la mesure où le gardien ne fait que maintenir la possession de données se trouvant légalement en sa possession et où les données ne sont divulguées aux responsables de la Partie requise ou examinées par eux qu'après l'exécution d'une demande d'entraide officielle visant leur divulgation. Ensuite, d'un point de vue pratique, il faut souvent tant de temps pour obtenir les éclaircissements nécessaires en vue d'établir de façon irréfutable l'existence de la double incrimination que les données pourraient être effacées, déplacées ou modifiées avant qu'elle puisse être établie. Ainsi, par exemple, aux premières étapes d'une enquête, la Partie requérante peut s'apercevoir qu'une intrusion dans un ordinateur se trouvant sur son territoire s'est produite, mais peut ne comprendre que plus tard la nature et l'étendue des dommages. Si la Partie requise devait ajourner la conservation des données relatives au trafic qui permettraient de remonter à la source de l'intrusion jusqu'à ce que la double incrimination ait été établie de façon irréfutable, les données décisives seraient souvent effacées par les fournisseurs de services qui ne les conservent

généralement que pendant quelques heures ou quelques jours après la transmission de la communication. Même si, par la suite, la Partie requérante était capable d'établir la double incrimination, les données décisives relatives au trafic ne pourraient pas être récupérées et l'auteur de l'infraction ne serait jamais identifié.

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

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

288. Il arrive que la Partie requise se rende compte que le gardien des données risque d'intervenir d'une façon qui compromette la confidentialité de l'enquête de la Partie requérante ou nuise d'une autre façon à celle-ci (par exemple lorsque les données à conserver sont sous la garde d'un fournisseur de services contrôlé par une organisation criminelle ou par la cible de l'enquête elle-même). En pareil cas, en vertu du paragraphe 6, la Partie requérante doit être rapidement informée, de sorte qu'elle puisse déterminer si elle peut prendre le risque que présente l'exécution de la requête de conservation ou s'il vaut mieux utiliser une forme plus intrusive mais plus sûre d'entraide, telle que l'injonction de produire ou la perquisition et la saisie.

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

7.4 Article 30 – Divulgation rapide de données conservées

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

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

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

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

Rapport explicatif:

Divulgation rapide de données conservées (article 30)

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

291. En vertu du paragraphe 2, la Partie requise ne peut refuser la divulgation de données relatives au trafic que si celle-ci risque de porter préjudice à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels, ou si elle considère l'infraction comme étant de nature politique ou liée à une infraction de nature politique. Comme pour l'article 29 (Conservation rapide de données informatiques stockées), ce type d'informations étant si important pour pouvoir identifier les auteurs d'infractions au sens de la Convention ou localiser des preuves décisives, les motifs de refus doivent être strictement limités, et il a été décidé d'interdire d'arguer de tout autre motif pour refuser une demande de divulgation.