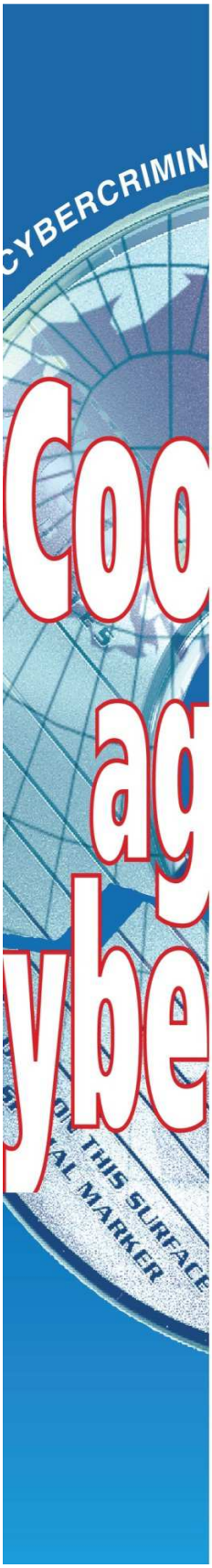

Comité de la Convention sur la cybercriminalité (T-CY)

Sous-groupe ad hoc sur la compétence et l'accès transfrontalier aux données et flux de données

Compétence et accès transfrontalier : quelles solutions ?

Rapport établi par le Groupe sur l'accès transfrontalier

adopté par le T-CY le 6 décembre 2012

T-CY (2012)3

Strasbourg, 6 décembre 2012 (provisoire)

www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Table des matières

Contact

Alexander Seger
Secrétariat du Comité de la Convention sur la cybercriminalité (T-CY)
Direction générale Droits de l'homme et Etat de droit
Conseil de l'Europe, Strasbourg, France

Tél. : +33-3-9021-4506
Fax : +33-3-9021-5650
E-mail : alexander.seger@coe.int

1 Introduction

1 Lors de sa 6e réunion plénière (23-24 novembre 2011), le Comité de la Convention sur la cybercriminalité (T-CY) a décidé de créer un « Sous-groupe ad hoc sur la compétence et l'accès transfrontalier aux données et flux de données[1] » (ci-après « Groupe sur l'accès transfrontalier »). Cette décision a été prise sur la base de l'article 46.1.a et c de la Convention de Budapest sur la cybercriminalité, aux termes duquel « les Parties[2] se concertent périodiquement, au besoin, pour faciliter […] l'usage et la mise en œuvre effectifs de la présente Convention » et « l'examen de l'éventualité de compléter ou d'amender la Convention[3] ». Le T-CY a confié au Groupe sur l'accès transfrontalier la mission

> d'élaborer un instrument tel qu'un amendement à la Convention, un protocole ou une recommandation visant à mieux réglementer l'accès transfrontalier aux données et aux flux de données, ainsi que le recours aux mesures d'enquêtes transfrontalières sur Internet et les questions y afférentes, et de soumettre cet instrument au Comité dans un rapport présentant ses conclusions.

2 Le Groupe devait examiner en particulier :

i. l'application de l'article 32b de la Convention sur la cybercriminalité,
ii. l'application de mesures d'enquête transfrontalières sur Internet,
iii. les défis que représentent, pour les enquêtes transfrontalières sur Internet, le droit international applicable concernant le ressort territorial et la souveraineté de l'État.

3 Le Groupe sur l'accès transfrontalier, dont le mandat expire le 31 décembre 2012, devait présenter son rapport au T-CY lors de la 2e réunion plénière de 2012 (prévue pour les 5 et 6 décembre).

4 Le Groupe sur l'accès transfrontalier s'est réuni pour la première fois à Strasbourg les 31 janvier et 1er février 2012, puis une deuxième fois du 1er au 3 juin 2012 à Klingenthal (près de Strasbourg) et les 26 et 27 septembre 2012 à Strasbourg. Il s'est appuyé sur les nombreux documents et informations transmis par les Parties à la Convention de Budapest[4], ainsi que sur les exposés et débats de la Conférence Octopus 2012[5].

5 Le Groupe s'est concentré sur l'accès transfrontalier aux données à des fins de justice pénale, c'est-à-dire ayant pour but d'enquêter sur des infractions visant des systèmes informatiques ou commises à l'aide de ces systèmes ou de recueillir des preuves électroniques d'une infraction

---

[1] http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY_2011_10F_plenrep.pdf
Le T-CY a décidé de nommer membres du Groupe sur l'accès transfrontalier : Ioana Albani (Roumanie), Andrea Candrian (Suisse), Markko Kunnapu (Estonie), Vladimir Miloseski (« ex-République yougoslave de Macédoine », qui s'est désisté par la suite), Erik Planken (Pays-Bas), Betty Shave (Etats-unis), Branko Stamenkovic (Serbie) et Pedro Verdelho (Portugal).

[2] Cette « concertation » se fait via le T-CY.

[3] Conformément à l'article 46.2, le rapport de la 6e réunion plénière du T-CY a été transmis au Comité européen pour les problèmes criminels (CDPC).

[4] Pour les références, se reporter à l'annexe (chapitre X.X).

[5] Voir le site Internet de la Conférence Octopus 2012, www.coe.int/octopus2012

pénale[6] dans le respect des principes des droits de l'homme et de la prééminence du droit. Le Groupe sur l'accès transfrontalier est ainsi resté dans le champ de la Convention de Budapest.

6 Le Groupe sur l'accès transfrontalier n'a pas étudié la question de l'accès aux données à des fins autres que les enquêtes pénales spécifiques et procédures pénales dans le cadre du champ d'application de l'article 14 de la Convention de Budapest.

7 Le rapport confirme la nécessité d'envisager un renforcement de l'accès transfrontalier compte tenu de l'évolution des technologies, tout en étudiant les préoccupations en matière de droits de l'homme et de prééminence du droit et les questions de souveraineté nationale que pourrait soulever un tel renforcement.

8 Le rapport s'attache à expliquer les dispositions actuelles de la Convention de Budapest, et en particulier son article 32. Il semblerait que davantage d'orientations soient requises de la part du T-CY pour permettre une meilleure compréhension de cet article.

9 Les pratiques actuelles d'accès direct des autorités répressives aux données et d'accès via des prestataires de services en ligne et d'autres entités privées sont examinées en détail. Elles montrent que dans de nombreux pays, les autorités répressives accèdent à des données stockées à l'étranger pour recueillir des preuves électroniques. Ces pratiques dépassent souvent les possibilités restreintes prévues à l'article 32b (Accès transfrontière avec consentement) et dans la Convention de Budapest en général.

10 Concernant les solutions possibles, le Groupe sur l'accès transfrontalier estime que les dispositions actuelles de la Convention de Budapest devraient être utilisées plus efficacement, que le T-CY devrait préparer une Note d'orientation sur l'article 32, mais aussi qu'il faudrait envisager la négociation d'un Protocole additionnel sur l'accès aux preuves électroniques.

11 Le présent rapport a été adopté lors de la 8ème Réunion Plenière du T-CY le 6 décembre 2012.

.

12 Le mandat du Groupe sur l'accès transfrontalier a été prolongé jusqu'au 31 décembre 2013 afin de pousuivre les deux options.

[6] Voir l'article 14 de la Convention.

2 Pourquoi revenir sur la question de l'accès transfrontalier ?

2.1 Historique

13 L'accès transfrontalier unilatéral, par les autorités répressives d'un territoire, à des données stockées dans un système informatique sur un autre territoire sans passer par l'entraide judiciaire est une question très complexe, puisqu'elle touche à des principes reconnus de droit international (en particulier le principe de territorialité, et donc la question de la souveraineté nationale) et aux garanties de procédure destinées à protéger les droits individuels.

14 La nécessité d'un accès transfrontalier aux preuves électroniques est débattue depuis les années 1980. Le problème de l'« intrusion directe », sous la forme soit d'une « intrusion directe pure », soit de l'ordre donné à une personne de produire des données stockées à l'étranger, a été soulevé dans la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur et dans le rapport final publié à ce sujet par le Comité européen pour les problèmes criminels (CDPC) en 1990[7]. A l'époque, le CDPC n'a pas formulé de propositions spécifiques, considérant que le moment n'était pas venu et que le problème n'avait pas encore un caractère urgent.

15 Cinq ans plus tard, en 1995, le Comité des Ministres du Conseil de l'Europe constate dans sa Recommandation R (95) 13[8] qu'il devient urgent de négocier un accord international sur ce thème :

> VII. Coopération internationale
> 17. Le pouvoir d'étendre la perquisition à d'autres systèmes informatiques devrait être également applicable lorsque le système se trouve sous une juridiction étrangère, à condition qu'une action immédiate soit requise. En vue d'éviter d'éventuelles violations de la souveraineté des Etats ou du droit international, une base légale explicite devrait être créée pour de telles perquisitions ou saisies étendues. Par conséquent, il y a un besoin urgent de négocier des instruments internationaux quant à la question de savoir comment, quand et dans quelle mesure de telles perquisitions ou saisies peuvent être permises.

16 En 2000, le préambule des premières versions de la Convention de Budapest mentionne explicitement les Recommandations R (89) 9 et R (95) 13, ainsi que le besoin de « réglementer les perquisitions et saisies transfrontalières[9] ».

17 Parallèlement aux négociations sur la Convention du Budapest, à partir de 1997, le G8 mène des discussions assez approfondies sur les solutions d'accès transfrontalier envisageables[10]. En octobre 1999, au cours de leur réunion à Moscou, les ministres de la Justice et de l'Intérieur du G8

---

[7] Rapport final, pages 86-89. http://www.oas.org/juridico/english/89-9&final%20Report.pdf

[8] « Recommandation relative aux problèmes de procédure pénale liés à la technologie de l'information », Rec(1995)013

[9] Par exemple la version provisoire n° 19 (avril 2000) : *« Rappelant la Recommandation n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, et la Recommandation n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information, qui appellent entre autres à négocier un instrument international pour réglementer les perquisitions et saisies transfrontalières ; ».* Le dernier passage a été abandonné dans les versions suivantes.

[10] Voir par exemple les propositions élaborées en 1997 par Donald Piragoff et Larissa Easson à l'attention du G8 et du Comité d'experts sur la criminalité dans le cyberespace (PC-CY), chargé d'élaborer la Convention de Budapest.

adoptent des « Principes sur l'accès transfrontalier aux données stockées dans des ordinateurs[11] ». Il est prévu notamment que les Etats autorisent des mesures comme la conservation rapide de données informatiques stockées[12] et l'entraide judiciaire rapide[13]. Les principes du G8 couvraient en outre « l'accès transfrontalier à des données informatiques sans entraide judiciaire » :

> Nonobstant les présents principes, un Etat n'a pas besoin d'obtenir l'autorisation d'un autre Etat lorsqu'il agit conformément à son droit national aux fins suivantes :
>
> accéder à des données publiquement disponibles (ouvertes), quel que soit l'emplacement géographique des données ;
>
> consulter, rechercher, copier ou saisir des données stockées dans un système informatique situé dans un autre Etat, si une personne régulièrement habilitée à divulguer ces données y a consenti volontairement et dans le respect des règles. L'Etat perquisitionneur devrait envisager d'avertir l'Etat perquisitionné, si son droit national autorise une telle notification et si les données révèlent une infraction pénale ou semblent présenter un intérêt pour l'Etat perquisitionné.

18 La structure et la teneur de ce principe adopté à Moscou est très proche de ce qui allait devenir l'article 32b de la Convention de Budapest, avec pour principale différence que l'idée d'« envisager d'avertir l'Etat perquisitionné » n'a pas été conservée.

19 Comme le montre ce bref aperçu, l'ouverture à la signature de la Convention de Budapest en novembre 2001 a été précédée de plus de seize ans de travaux préparatoires au Conseil de l'Europe et dans d'autres cadres[14]. La question de l'accès transfrontalier était présente dans les délibérations dès le début. Avec l'article 32b, une exception au principe de territorialité, dans des conditions très strictes, a finalement été adoptée.

20 Les auteurs de la Convention ne jugeaient pas exclu de prévoir d'autres possibilités d'accès transfrontalier. Comme remarqué au paragraphe 293 du Rapport explicatif,

- Les Parties ont décidé de poursuivre la discussion et de réglementer des situations autres que celles prévues à l'article 32 ultérieurement, après avoir acquis davantage d'expérience.

- Les situations d'accès transfrontalier autres que celles figurant dans l'article 32 ne sont « ni autorisées ni exclues ».

21 Le T-CY a rouvert une discussion sur ce sujet en octobre 2009, en étudiant les expériences des Etats parties concernant l'accès transfrontalier aux données sur la base de réponses à un questionnaire[15].

22 Cette initiative a amené le T-CY, les 23 et 24 novembre 2011, à mettre en place le Groupe sur l'accès transfrontalier, chargé d'étudier les nouvelles possibilités de réglementation dans ce domaine.

---

[11] Publiés lors de la Conférence ministérielle des pays du G8 sur la lutte contre la criminalité transnationale organisée, Moscou, 19-20 octobre 1999.

[12] Principes détaillés plus tard dans les articles 16, 17, 29 et 30 de la Convention de Budapest.

[13] Principe repris plus tard dans l'article 31 de la Convention de Budapest.

[14] Le Comité restreint d'experts sur la criminalité en relation avec l'ordinateur, qui a préparé la Recommandation R (89) 9, avait été créé en mars 1985.

[15] Document T-CY(2010)01.

2.2 Nécessité de l'accès transfrontalier

2.2.1 Nécessité d'accéder à des données à des fins de justice pénale

23 L'usage des technologies de l'information et de la communication (TIC) a connu une augmentation exponentielle ces dix dernières années. Selon les estimations par exemple, fin 2011, le nombre de personnes utilisant Internet dans le monde s'élevait à plus de 2,3 milliards et le nombre d'abonnements à la téléphonie mobile atteignait presque 6 milliards[16].

24 L'expansion de l'usage des TIC dans le monde entier s'accompagne d'un accroissement des infractions visant des systèmes informatiques ou commises au moyen de systèmes informatiques. En outre, il est de plus en plus fréquent que des données stockées dans un système informatique servent à apporter la preuve d'une infraction, quelle qu'elle soit.

25 Les gouvernements ont l'obligation positive de protéger les droits individuels, entre autres à travers une législation pénale et des mesures destinées à la faire appliquer[17]. La collecte de preuves joue ici un rôle essentiel. Poursuivre les auteurs d'infractions ou prouver l'innocence de suspects constitue l'objectif premier de toute enquête pénale. C'est pourquoi la Convention de Budapest comprend une série de mesures procédurales visant à assurer la détection, la perquisition, la saisie ou l'interception de données électroniques et d'autres moyens de preuve. Ces mesures procédurales s'appliquent aux preuves électroniques de toute infraction pénale[18].

26 Les autorités répressives, c'est-à-dire les procureurs, enquêteurs et policiers autorisés à appliquer ces mesures peuvent avoir besoin d'accéder à un large éventail de preuves électroniques :

- tout type de donnée informatique, notamment des contenus (documents, images, e-mails, souvent encodés), des programmes, des données relatives au fonctionnement du système etc.[19] ;
- tout type de donnée relative au trafic, concernant par exemple la source, la trajectoire et la destination d'une communication, le type de service de communication utilisé, la début et la fin d'une session Internet, les services utilisés, le nom et les coordonnées d'un utilisateur auquel une adresse de protocole Internet (IP) a été attribuée au moment de la communication, etc.[20].

27 Les preuves électroniques peuvent se trouver sur tout type de système informatique[21] : ordinateurs centraux, PC, ordinateurs portables ; téléphones portables, tablettes etc. ; réseaux

[16] Source : http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf

[17] Comme souligné également par la Cour européenne des droits de l'homme, par exemple dans l'arrêt *K.U. c. Finlande* (n° 2872/02, décembre 2008), qui cite la Convention de Budapest, en particulier concernant les mesures procédurales. http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90015

[18] Voir l'article 14.

[19] Voir la définition large de l'expression « données informatiques » à l'article 1 de la Convention de Budapest.

[20] Voir la définition des « données relatives au trafic » à l'article 1 de la Convention de Budapest.

[21] Voir la définition de « système informatique » à l'article 1 de la Convention de Budapest. Lors de sa première réunion, en 2006, le T-CY a convenu de donner un sens large à cette définition, englobant les téléphones portables et les autres équipements capables de créer, de traiter et de transmettre des données. Voir le rapport de réunion, p. 2 : http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY%20(2006)%2011%20E.pdf

informatiques et matériel associé comme les hubs, routeurs, serveurs etc. ; systèmes de stockage comme les disques durs, clés USB, cartes mémoire etc. ; périphériques ; enregistreurs audio/vidéo, diffuseurs de médias portables, consoles de jeu et autres.

28 L'« accès » peut recouvrir la conservation et la divulgation partielle de données de trafic (article 17 de la Convention de Budapest), la perquisition et la saisie (article 19), des injonctions de produire ou de divulguer (article 18), mais aussi la collecte en temps réel de données de trafic (article 20) ou l'interception de données de contenu (article 21). La conservation rapide des données (article 16) est une mesure provisoire permettant de faciliter les perquisitions, saisies ou communications régulières.

29 Devant l'évolution des technologies, certaines autorités répressives jugent qu'il leur faudra de plus en plus intercepter à la source des données et des communications (y compris la voix transmise par IP), obtenir des mots de passe, installer des programmes sur les systèmes des suspects ou appliquer d'autres mesures coercitives pour accéder aux ordinateurs ou aux données de suspects. Ces propositions ne sont pas toutes susceptibles de faire consensus au niveau international.

30 La question est de savoir comment des preuves électroniques peuvent être recueillies et quelles mesures sont applicables si les ordinateurs et les données se situent physiquement à l'étranger, en lieu inconnu ou en plusieurs lieux à la fois ou s'ils changent constamment de territoire.

2.2.2 Evolutions technologiques

31 Les technologies et les modes d'utilisation des ordinateurs – y compris par des criminels – ont considérablement évolué ces dernières années. Pour les autorités répressives, cela pose toute une série de défis :

- Le volume de données sauvegardées, traitées et transmises augmente.
- Les individus peuvent utiliser non plus un mais plusieurs équipements, simultanément ou successivement.
- Les cybercriminels ont appris à encoder leurs données ou à rester anonymes lorsqu'ils utilisent les TIC (utilisation de serveurs proxy, de routeurs TOR, d'IP étrangères, d'encodage de la voix etc.).
- Les ordinateurs d'usagers innocents sont détournés et utilisés à des fins malveillantes (« réseaux zombies »).
- Des infractions sont commises à distance, depuis des Etats tiers, ou via les infrastructures d'information d'un Etat tiers pour ne pas attirer l'attention des enquêteurs.
- Même lorsqu'une personne commet une infraction dans son propre pays, les preuves électroniques (données stockées, services Internet utilisés, données d'acheminement des communications) peuvent relever de beaucoup d'autres ressorts.
- Les données, y compris les preuves électroniques, sont de plus en plus évanescentes. En quelques secondes, on peut changer l'adresse IP d'un site Internet ou d'une URL contenant des données illégales et des preuves électroniques.
- On observe un essor de l'informatique décentralisée ou « en nuage » (*cloud computing*) et des services Internet où les données (preuves électroniques comprises) sont stockées « quelque part en ligne », c'est-à-dire sur un ou plusieurs serveurs – qui parfois changent au fil du temps – qui se trouvent dans des lieux et des ressorts territoriaux souvent inconnus des usagers comme des autorités répressives.

32 Il faut donc trouver des solutions pour que les autorités répressives puissent mettre la main sur des preuves qui sont évanescentes, instables et éparpillées dans de très nombreux pays.

33 Par ailleurs, dans des circonstances exceptionnelles, les autorités répressives de la plupart des Etats peuvent – dans le cadre d'enquêtes nationales – prendre des mesures immédiates pour empêcher un risque imminent pour la vie, l'intégrité physique ou les biens, l'évasion d'un suspect ou la destruction de preuves. Dans ces situations, les autorités peuvent agir de façon extrajudiciaire. Cela peut aussi s'appliquer à la perquisition ou à la saisie de preuves électroniques, si ces preuves risquent d'être perdues ou dans d'autres circonstances exceptionnelles[22].

34 La question est de savoir si et à quelles conditions le recueil de preuves électroniques ou les autres mesures exceptionnellement autorisées en droit national pourraient être autorisés dans des situations internationales où les données sont stockées à l'étranger ou dans un lieu inconnu.

2.2.3 La « disparition du lieu »

35 Les dernières évolutions technologiques, et en particulier le stockage décentralisé, ont peut-être entraîné la « disparition du lieu[23] ». Les données passent d'un serveur ou d'un ressort territorial à l'autre ou peuvent être dupliquées, pour des raisons de sécurité et de disponibilité, relevant ainsi de plusieurs ressorts à la fois. Un site Internet peut se composer d'un réseau de sources d'informations reliées entre elles et qui ne cessent d'évoluer[24].

36 Le pouvoir de rechercher des preuves électroniques, notamment au moyen de mesures coercitives, est habituellement lié à un lieu spécifique. Le lieu détermine quelles autorités peuvent enquêter et appliquer des mesures coercitives et sur quelle base juridique. Il aide aussi à déterminer les droits des suspects ou des parties lésées. Si les données sont stockées dans un seul Etat, les autorités répressives peuvent appliquer les pouvoirs qui leur sont conférés par le droit national.

37 Si les données sont stockées dans un autre pays, les autorités doivent recourir à la coopération internationale. La règle fondamentale en droit international concernant l'exercice de pouvoirs coercitifs est le principe de la souveraineté territoriale. Aucun Etat ne peut faire appliquer ses lois sur le territoire d'un autre Etat souverain[25]. Par conséquent, la coopération internationale repose sur des traités internationaux – comme la Convention de Budapest sur la cybercriminalité – ou sur des accords bilatéraux entre les Etats concernés.

38 Dans le contexte du stockage décentralisé et des services en ligne, le lieu n'est pas fixe. Le concept de données stockées dans un système informatique en un lieu ou sur un territoire donné a peut-être perdu de sa pertinence. Cela soulève d'importantes questions sur la valeur du principe de territorialité comme critère de définition des autorités compétentes.

2.2.4 Accès via des prestataires et autres entités privées

39 Au lieu d'accéder à des données stockées à l'étranger directement ou par le biais de l'entraide judiciaire internationale, les autorités répressives peuvent s'adresser à des prestataires de services

[22] Pour les Etats-Unis, voir le document suivant, à partir de la p. 27 : http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf

[23] Voir : http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

[24] Sansom, Gareth (2008), « Website Location: Cyberspace vs. Geographic Space » (3 avril 2008), disponible sur http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/t-cy/Gareth%20Samson%20Website%20Location.pdf

[25] Voir l'affaire du « Lotus » (France c. Turquie), CPIJ série A, n° 10.

Internet ou à d'autres entités du secteur privé, soit par l'intermédiaire de la représentation juridique de ces entités dans leur pays, soit éventuellement en contactant l'entité à l'étranger.

40 Il a été avancé qu'un tel accès pouvait porter atteinte à la souveraineté de l'autre Etat, à moins que ce dernier n'ait donné son accord[26].

41 Les scénarios, pratiques et problèmes actuels et les solutions possibles seront abordés plus en détail dans la suite du rapport.

2.2.5 Conclusion : nécessité de solutions communes

42 Les dispositions de la Convention de Budapest sur la cybercriminalité restent valables, même si les technologies ont évolué et si le rôle des TIC dans nos sociétés s'est encore accru. La mise en œuvre effective des outils et dispositions de procédure en matière de coopération internationale aidera à répondre à beaucoup des défis évoqués ci-dessus.

43 Concernant le thème spécifique de l'accès transfrontalier aux données, deux articles sont particulièrement pertinents : l'article 19.2, qui permet à chaque Partie de consulter les systèmes informatiques accessibles « sur son territoire » à partir du système initial, et l'article 32, qui couvre l'accès transfrontalier aux données publiques (32a) et l'accès transfrontalier avec consentement (32b).

44 Comme on le verra dans ce rapport, dans plusieurs pays, la législation et les pratiques dépassent ces dispositions pour ce qui est de l'accès transfrontalier direct ou de l'accès via des entités privées. Les pratiques semblent varier considérablement d'un pays à l'autre.

45 Afin de mieux orienter les Etats parties à la Convention de Budapest, il semble donc nécessaire de formuler des solutions communes.

2.3 Impact sur les droits de l'homme et la prééminence du droit

46 La criminalité porte atteinte aux droits individuels. Cela vaut aussi pour la cybercriminalité. Une attaque visant la confidentialité, l'intégrité et la disponibilité des systèmes et données informatiques (articles 2 à 6 de la Convention de Budapest), par exemple, porte atteinte à la vie privée et à d'autres droits. Comme le souligne la Cour européenne des droits de l'homme, les gouvernements ont donc l'obligation positive de protéger les droits individuels, entre autres à travers une législation pénale et des mesures destinées à la faire appliquer, y compris celles prévues par la Convention de Budapest[27]. Dans le même temps, les enquêtes sur les affaires de cybercriminalité doivent elles aussi respecter les droits individuels[28].

47 Par conséquent, et bien que les ordinateurs et Internet aient aidé la criminalité à dépasser les frontières, il y a des raisons de se montrer prudent avant d'élargir les conditions d'accès transfrontalier par les autorités répressives. Bien que les Etats partagent beaucoup de points de vue sur des questions comme la protection des personnes ou celle des intérêts légitimes des tiers, les régimes qu'ils appliquent diffèrent encore beaucoup sur le plan juridique et pratique. Beaucoup

[26] Sieber 2012 : C147/148.

[27] Voir par exemple l'arrêt *K.U. c. Finlande* (n° 2872/02, décembre 2008), qui cite la Convention de Budapest, en particulier concernant les mesures procédurales.
http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90015

[28] Voir l'article 15 de la Convention de Budapest, « Conditions et sauvegardes ».

des obstacles et difficultés qui ont empêché un consensus allant au-delà de l'article 32b peuvent encore exister aujourd'hui.

2.3.1 Préoccupations juridiques et politiques pour les Etats

48 La coopération internationale en matière pénale repose sur plusieurs principes, dont la reconnaissance de l'infraction dans les deux pays (« double incrimination ») ou la possibilité de refuser la coopération si elle est contraire à l'ordre interne de l'Etat requis. L'accès transfrontalier peut être utilisé pour contourner de tels principes.

49 Supposons par exemple que la police d'un pays A soupçonne un ressortissant d'un pays B d'avoir commis un acte qui constitue un crime sur son territoire mais non sur celui du pays B. Si la police du pays A se rend dans le pays B pour recueillir des preuves contre cette personne, cela peut poser d'importants problèmes juridiques et politiques pour le pays B. Dans un premier temps, le pays B pourrait subordonner son aide au respect du principe de double incrimination, soit de façon générale soit en vertu d'accords de coopération (signés avec des pays aux systèmes juridiques très différents du sien). Même sans exiger le respect de ce principe, il peut se réserver le droit de refuser son aide lorsqu'il juge que cela serait contraire à son ordre interne. Par exemple, le pays B, qui reconnaît une large liberté d'expression, peut s'opposer à ce que le pays A vienne chercher sur son territoire des preuves d'un comportement diffamatoire qui serait légal selon son propre système juridique. Il pourra justifier son objection par le fait que la diffamation n'est pas une infraction pénale chez lui ou qu'une telle coopération serait contraire à son ordre interne.

50 Il peut aussi arriver que la police du pays B mène ses perquisitions selon d'autres règles que celles appliquées dans le pays A et puisse faire l'objet de sanctions pénales, civiles ou administratives en cas de manquement à ces règles. Pour le pays B, il peut être difficile sur le plan juridique ou politique d'autoriser le pays A à fouiller directement des systèmes informatiques relevant de son ressort selon des règles qui diffèrent des siennes.

51 On voit donc, avant même de passer à l'examen des questions ci-dessous, que l'élaboration d'un régime de perquisitions transfrontalières allant au-delà de l'article 32 soulève d'épineuses difficultés juridiques et politiques.

2.3.2 Conséquences pour les individus

52 L'accès transfrontalier soulève un problème majeur : il est difficile, pour les autorités étrangères, d'appliquer les règles de protection des droits individuels en vigueur dans l'Etat où se trouve le système informatique perquisitionné. Il y a consensus pour dire que l'accès transfrontalier doit protéger les individus en s'accompagnant de conditions et de garanties applicables aux perquisitions informatiques et en ligne de la part des autorités répressives[29]. Cependant, les Etats divergent quant aux garanties et protections à appliquer. Les différences dans l'étendue de la liberté d'expression ou dans les conditions à remplir par la police pour obtenir l'autorisation de perquisitionner comptent parmi les exemples les plus connus. Les habitants[30] d'un pays donné

[29] Voir l'article 15 de la Convention sur la cybercriminalité et les passages du Rapport explicatif à ce sujet. Les mêmes principes devraient valoir pour tous les types d'accès aux données par des autorités répressives. Pour une analyse de l'article 15 de la Convention sur la cybercriminalité, voir http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf.

[30] Dans le contexte de ce chapitre, on entend par « habitants » à la fois les personnes physiques et morales, dans la mesure où les personnes morales bénéficient des droits et garanties présentées ici.

s'attendent à juste titre à bénéficier au moins des garanties prévues dans leur pays, et non à subir des perquisitions conformément aux règles d'un pays dans lequel ils ne vivent pas et où ils ne se sont parfois jamais rendus. L'Etat, pour sa part, est tenu de respecter les droits et libertés individuels énoncés dans sa législation. La question est donc : en cas d'accès transfrontalier, quel est l'Etat dont les conditions et garanties s'appliquent ?

53 L'accès transfrontalier peut aussi soulever d'importantes questions juridiques et politiques lorsqu'une autorité répressive recueille des preuves selon des modalités qui sont illégales dans l'Etat où se trouvent les données. Outre les exemples déjà cités, un pays G peut interdire l'interception des communications électroniques et ne pas souhaiter qu'un pays F puisse procéder à des interceptions transfrontalières. Un pays H peut permettre à un procureur d'ordonner une perquisition tandis que dans le pays I, ce n'est possible qu'en vertu d'un mandat judiciaire.

54 L'endroit où se trouve la personne et le lieu de l'infraction peuvent changer la donne. Les préoccupations peuvent être moindres si la personne et l'infraction se situent dans le même Etat, seules les données étant localisées dans un autre. Du moment que les autorités répressives respectent les conditions et les garanties de leur propre législation nationale, l'intéressé sera correctement protégé.

55 Par ailleurs, l'élargissement des perquisitions transfrontalières peut prêter à des abus de la part d'Etats moins soucieux de la prééminence du droit. Par exemple, l'accès transfrontalier peut être utilisé, sous couvert d'action répressive légitime, pour mener des enquêtes abusives sur des dissidents politiques et mettre un terme à des activités politiques légitimes. Un pays J peut considérer un blogueur comme un dissident politique digne de sympathie alors que pour le pays K, il incite au trouble à l'ordre public ou même au terrorisme.

56 Comme on le voit, l'accès transfrontalier soulève de nombreux problèmes pour la protection des individus concernés. Pour le dire simplement, les habitants d'un pays s'attendent à bénéficier de garanties prévisibles. Lever les inquiétudes liées à l'application de conditions et de garanties de pays différents sera une étape aussi difficile que nécessaire dans les discussions sur le renforcement de l'accès transfrontalier.

57 Les actions des autorités répressives d'Etats parties à la Convention européenne des droits de l'homme peuvent être contestées devant la Cour européenne des droits de l'homme comme constituant l'exercice d'une juridiction extraterritoriale, contraire à l'article 1[31]. Les personnes affectées par de telles actions peuvent donc bénéficier du régime de protection de la Convention européenne des droits de l'homme.

2.3.3 Conséquences pour les tiers

58 L'accès transfrontalier peut aussi avoir un impact sur les droits des tiers, dont notamment les gestionnaires de systèmes et les prestataires de services. Ces tiers s'attendent à pouvoir travailler dans le cadre des règles de l'Etat où ils se trouvent et où ils exercent leur activité. Les Etats ont mis en place des conditions et garanties sur les perquisitions informatiques et en ligne qui tiennent compte des intérêts légitimes des tiers[32]. Cependant, l'accès transfrontalier peut mettre ces tiers dans une situation délicate, sur le plan à la fois juridique et pratique.

[31] http://www.echr.coe.int/NR/rdonlyres/D34FA717-6018-44F6-BC26-1274E401982E/0/FICHES_Juridiction_Extraterritoriale_FR.pdf

[32] Voir l'article 15.3 de la Convention sur la cybercriminalité et le passage du Rapport explicatif à ce sujet.

59 Les prestataires de services Internet, toutes les entreprises dotées de sites Internet pouvant être utilisés depuis d'autres pays et les autres tiers détenant des données au sujet d'une personne ou pour son compte ont déjà le plus grand mal à respecter les législations hétérogènes et parfois contradictoires d'Etats différents. Aux Etats-Unis par exemple, pour un prestataire de services commerciaux, divulguer à quiconque (y compris à un gouvernement étranger) le contenu d'une communication électronique constitue généralement une infraction pénale[33]. En France, la législation interdit à tout ressortissant français, à toute personne résidant habituellement sur le territoire français et à tout représentant d'une personne morale y ayant son siège ou un établissement de communiquer à des autorités publiques étrangères des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public[34].

60 Pourtant, des prestataires de services français ou étasuniens peuvent recevoir d'autres pays des injonctions de produire de telles informations. L'application directe de législations étrangères, y compris en matière de confidentialité, est lourde de conséquences pour les prestataires de services, où qu'ils se trouvent. Le renforcement de l'accès transfrontalier est susceptible de compliquer encore davantage la vie de ces entreprises.

61 Etant donné que le renforcement de l'accès transfrontalier aurait des répercussions sur des entités du secteur privé et sur d'autres acteurs, il conviendrait de recueillir l'avis des acteurs privés et de la société civile au moment de négocier des instruments supplémentaires.

2.3.4 Risques pour la protection des données personnelles

62 De plus en plus d'entités privées, dont des prestataires de services décentralisés, conservent des données personnelles. Le fait que des autorités répressives étrangères accèdent à de telles données ou qu'elles leur soient divulguées peut porter atteinte à la réglementation en matière de protection des données.

63 Dans la mesure où les adresses IP sont considérées comme des données personnelles, cela s'applique aussi aux données de trafic.

64 Ce risque a été souligné par le Groupe de travail « article 29 » de l'UE :

> Manque de confidentialité concernant les demandes adressées par les services répressifs directement aux fournisseurs d'informatique en nuage : les données à caractère personnel traitées dans le nuage peuvent faire l'objet de demandes de la part des organes répressifs des États membres de l'UE et des pays tiers. Les données à caractère personnel risquent d'être communiquées à des organes répressifs (étrangers) sans que cette communication ne soit fondée sur une base juridique en vigueur dans l'UE, ce qui entraînerait une violation de la législation de l'Union européenne en matière de protection des données[35].

65 Le cadre européen en matière de protection des données est actuellement en cours de réforme. Le Conseil de l'Europe travaille à moderniser sa Convention sur la protection des données à caractère

[33] Code des Etats-Unis, Titre 18, article 2701, disponible sur : http://uscode.house.gov/download/title_18.shtml

[34] Loi du 26 juillet 1968, modifiée par la loi du 17 juillet 1980 et par l'ordonnance du 19 septembre 2000, disponible sur : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326

[35] Groupe de travail « article 29 » sur la protection des données (2012) : « Avis 05/2012 sur l'informatique en nuage », adopté le 1er juillet 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf

personnel (n° 108[36]). En janvier 2012, la Commission européenne a présenté son « dispositif sur la protection des données », c'est-à-dire un Règlement général directement applicable[37] et une Directive couvrant la protection des données dans le domaine de la justice pénale[38]. Les versions provisoires de ces deux documents sont en cours d'examen.

66 Concernant l'accès à des données via des prestataires ou d'autres entités privées, le considérant n° 90 du projet de Règlement est rédigé comme suit :

> (90) Certains pays tiers édictent des lois, des règlements et d'autres instruments législatifs qui visent à régir directement des activités de traitement des données effectuées par des personnes physiques et morales qui relèvent de la compétence des Etats membres de l'Union. L'application extraterritoriale de ces lois, règlements et autres instruments législatifs peut être contraire au droit international et faire obstacle à la protection des personnes garantie dans l'Union par le présent règlement. Les transferts ne devraient donc être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies. Ce peut être le cas, notamment, lorsque la divulgation est nécessaire pour un motif important d'intérêt général reconnu par le droit de l'Union ou par le droit d'un Etat membre auquel le responsable des données est soumis. Les critères d'existence d'un motif important d'intérêt général devraient être précisés par la Commission dans un acte délégué.

67 Une limitation de l'utilisation des données peut aussi s'avérer nécessaire. Si une entreprise transfère des données vers un autre pays pour des raisons techniques ou à d'autres fins légitimes, puis se voit contrainte par la législation de ce pays de divulguer des données aux autorités répressives, il peut y avoir violation des règles de protection des données du pays d'origine.

68 Certains craignent que les projets de Règlement et de Directive ne nuisent à l'efficacité de la coopération entre autorités répressives et qu'ils n'obligent à renégocier des accords internationaux[39] :

> Article 60 [projet de Directive] – Relation avec les accords internationaux conclus antérieurement dans le domaine de la coopération judiciaire en matière pénale et de la coopération policière
>
> Les accords internationaux conclus par les Etats membres avant l'entrée en vigueur de la présente directive sont modifiés, en tant que de besoin, dans un délai de cinq ans à compter de son entrée en vigueur.

69 Cela pourrait aussi concerner la Convention de Budapest, qui oblige ses Parties à coopérer « dans la mesure la plus large possible » (article 23) et qui restreint les motifs de refus d'entraide. Le

[36] www.coe.int/dataprotection

[37] « Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données) » (Bruxelles, 25 janvier 2012, COM (2012) 11 final), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf

[38] « Proposition de Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel pour les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation des données » (Bruxelles, 25 janvier 2012, COM(2012) 10 final), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:FR:PDF

[39] Craintes exprimées par exemple lors de la réunion de la Commission interparlementaire sur le thème « La réforme du cadre de la protection des données dans l'Union – Inspirer la confiance dans un monde numérique et global », Parlement européen, Bruxelles, 9 et 10 octobre 2012.

Rapport explicatif (paragraphe 269) précise que « le refus d'entraide au motif de la protection des données ne peut être invoqué que dans des cas exceptionnels ».

70 L'évolution du cadre de protection des données de l'Union européenne devra être prise en compte au moment d'étudier, en général, les moyens de rendre plus efficace la coopération internationale contre la cybercriminalité et en particulier les solutions supplémentaires d'accès transfrontalier aux données.

2.3.5 Risques pour les biens

71 L'intervention d'autorités répressives dans un réseau informatique étranger pose des problèmes pratiques, notamment concernant les moyens d'entrée, l'accès aux données privées ou protégées et la protection des consommateurs. Non seulement cette autorité étrangère peut être amenée à examiner les données d'un réseau informatique tiers, ce qui est déjà assez inquiétant si cet examen n'est pas légitime, mais ses actions peuvent endommager des données ou le système lui-même. Tout renforcement de l'accès transfrontalier devrait tenir compte des risques pour les biens, y compris pour la propriété intellectuelle[40].

2.3.6 Risques pour les opérations répressives

72 En plus d'affecter les individus et les tiers, l'accès transfrontalier peut représenter un risque pour les opérations répressives nationales et internationales. Une enquête repose souvent sur le secret et sur la coopération de tierces parties. L'accès transfrontalier peut poser des problèmes de coordination, rendre certaines données indisponibles pour des autorités nationales ou avoir pour conséquence d'avertir un suspect de l'enquête en cours. Comme c'est déjà arrivé, les autorités répressives d'un même pays ou de pays différents peuvent se retrouver à enquêter les unes sur les autres pour avoir confondu des opérations répressives légitimes avec des activités criminelles.

2.3.7 Conclusion : nécessité de garanties et de procédures limitant l'accès transfrontalier

73 Les solutions visant à protéger les individus, les tiers ou les opérations des autorités répressives devront surmonter les difficultés pratiques liées à l'assouplissement des règles de l'accès transfrontalier. Les Etats participants devront s'accorder sur les conditions et garanties minimales qui s'appliquent lorsqu'une autorité répressive intervient dans un autre Etat pour obtenir des informations électroniques. Les Etats doivent élaborer et adopter des procédures applicables à la coordination de l'accès transfrontalier et à la communication entre eux concernant ces activités. Il faudra tenir compte, tout particulièrement, des lois et procédures nationales de l'Etat où se trouvent les données ou la personne visée, y compris en matière de protection des données. Pour accepter un accès transfrontalier, un Etat doit être convaincu que l'accès sera conforme à des lois et politiques essentielles, allant de la protection des droits individuels par sa Constitution aux dispositions pénales en matière d'informatique et de réseaux en passant par la protection de la propriété privée. Les Etats doivent aussi s'accorder sur des mécanismes de mise en œuvre capables de dissuader les usages abusifs de l'accès transfrontalier.

---

[40] Cette question relève de l'article 1 du Protocole additionnel n° 1 à la Convention européenne des droits de l'homme. Voir en particulier le rapport « Internet : la jurisprudence de la Cour européenne des droits de l'homme », Division de la Recherche de la Cour, 2011, disponible sur http://www.echr.coe.int/NR/rdonlyres/93F136C4-77BC-4A6E-8B42-814F9D029C78/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_FR.pdf

74 A terme, le renforcement de l'accès transfrontalier supposera que les Etats abandonnent une part de souveraineté. Avant qu'ils ne le fassent, il faudra résoudre les difficultés juridiques et pratiques évoquées ci-dessus, ce qui ne s'est pas avéré possible à ce jour. Quelles que soient l'urgence et l'importance d'améliorer la capacité des autorités répressives à enquêter sur les infractions pénales facilitées par l'informatique et Internet et à en poursuivre les auteurs, les Etats devront avoir l'assurance que leurs intérêts et ceux de leurs habitants seront à l'abri d'accès abusifs de la part d'autres Etats.

3 Explication des dispositions pertinentes de la Convention de Budapest

3.1 Aperçu

75 La Convention de Budapest demande aux Parties :

- d'ériger en infractions pénales les atteintes à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques (articles 2-6) et les infractions commises par le biais de l'informatique (articles 7-10), de couvrir les responsabilités auxiliaires et de les sanctionner (articles 11-13) et d'établir leur compétence à l'égard des infractions pénales visées aux articles 2 à 11 (article 22) ;

- d'établir des procédures judiciaires permettant de rechercher et d'établir efficacement des preuves électroniques, comme la perquisition et la saisie de données informatiques, leur conservation, leur collecte en temps réel ou leur interception (articles 16-21) ;

- de mener une coopération internationale efficace (articles 23-35).

76 La Convention reprend d'une part des mesures procédurales traditionnelles, en les adaptant au nouvel environnement technologique. D'autre part, elle crée de nouvelles méthodes, comme la conservation rapide des données[41], pour veiller à ce que les mesures procédurales restent efficaces dans un environnement électronique instable.

77 Certaines des mesures procédurales à adopter au niveau national sont reprises dans le chapitre sur la coopération internationale[42], afin de veiller à ce que cette coopération s'avère efficace pour établir des preuves.

78 L'article 14 prévoit un large champ d'application pour les mesures procédurales : leur application n'est pas limitée à la poursuite des infractions pénales mentionnées dans la Convention. Cet article oblige expressément les Parties à appliquer ces pouvoirs et procédures à toutes les infractions pénales commises au moyen d'un système informatique et à la collecte de preuves électroniques. Ce champ d'application large vaut aussi – avec des exceptions – pour la coopération internationale[43]. Le texte de la Convention précise bien que les Etats devraient prévoir en droit national la possibilité et les moyens de veiller à ce que les informations sous forme électronique puissent être utilisées comme preuves devant les juridictions pénales, quelle que soit la nature de l'infraction pénale concernée[44].

79 En vertu de l'article 15, la mise en œuvre et l'application des mesures procédurales sont soumises aux conditions et sauvegardes prévues en droit interne[45]. L'objectif est de protéger correctement

[41] Articles 16 et 17 de la Convention.

[42] L'article 16 (conservation rapide) est repris à l'article 29, l'article 17 (divulgation partielle) à l'article 30, l'article 20 (collecte en temps réel de données relatives au trafic) à l'article 33 et l'article 21 (interception du contenu) à l'article 34.

[43] Voir le paragraphe 243 du Rapport explicatif.

[44] Voir aussi le paragraphe 141 du Rapport explicatif.

[45] Pour une analyse de l'article 15, voir http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

les droits de l'homme et les libertés fondamentales, tels que les droits et obligations découlant de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950) ou d'autres instruments internationaux de droits de l'homme. Le principe de proportionnalité doit être respecté. C'est aux Parties qu'il revient de déterminer quels pouvoirs et procédures ont un caractère suffisamment intrusif pour justifier l'application de garanties supplémentaires pour la protection des droits fondamentaux.

80 Conformément à l'article 15.3, les Etats doivent examiner l'effet de leurs mesures procédurales sur les droits, responsabilités et intérêts des tiers. Des moyens peuvent être mis en œuvre pour réduire ces effets : réglementation des responsabilités en cas de divulgation de données, protection des intérêts patrimoniaux ou protection des intérêts des prestataires de services, par exemple[46].

81 Voici donc les points importants à retenir :

- la Convention de Budapest prévoit une série de mesures permettant d'établir efficacement des preuves électroniques de toute infraction pénale, au niveau national et international ;

- les enquêtes sur la cybercriminalité et les actions visant à établir des preuves électroniques doivent respecter les principes des droits de l'homme et de la prééminence du droit.

82 Confrontées à des crimes comportant des éléments transnationaux, les autorités nationales en charge des poursuites ont besoin de moyens rapides, fiables et efficaces d'obtenir des preuves et des informations depuis l'étranger. Ces moyens doivent être légaux, afin que les preuves obtenues puissent être utilisées devant un tribunal. La procédure classique dans ce domaine est l'entraide judiciaire.

83 La Convention de Budapest, aux articles 23 à 35, comprend une série de dispositions générales ou plus spécifiques sur la coopération internationale en matière de cybercriminalité et de preuves électroniques. Son approche associe à l'entraide judiciaire classique plusieurs mesures provisoires destinées à établir rapidement des preuves électroniques (articles 29 et 30 combinés à l'article 35, consacré à leur mise en œuvre pratique).

84 Le principe de subsidiarité s'applique : les Parties sont censées coopérer sur la base des accords bilatéraux ou multilatéraux existants, la Convention de Budapest venant les compléter ou les remplacer s'ils n'existent pas. Les accords sur le même sujet ne doivent pas contredire les principes de la Convention de Budapest (articles 23 et 39). En revanche, les parties peuvent aller au-delà des dispositions de la Convention en matière de coopération internationale.

85 Les discussions qui ont eu lieu avant, pendant et après les négociations sur la Convention de Budapest ont souligné, compte tenu des préoccupations concernant la souveraineté nationale et les droits individuels de procédure et de respect de la vie privée, qu'il fallait en premier lieu rendre

[46] Voir aussi le paragraphe 148 du Rapport explicatif.

l'entraide judiciaire plus efficace, en se concentrant sur les mesures spécifiques prévues aux articles 29 à 34[47].

86 Par ailleurs, dans le cyberespace, les frontières et délimitations de compétences nationales peuvent ne pas être reconnaissables. Souvent, les autorités répressives qui accèdent à des données stockées via un réseau électronique ne sont pas en mesure de déterminer si un ensemble spécifique de données se trouve physiquement dans l'Etat d'où elles se connectent à Internet ou dans un autre Etat. Le recours croissant à des hébergeurs Internet extérieurs et à des outils et services décentralisés complique encore la situation.

87 L'article 32, sur l'accès transfrontalier, a permis de définir dans le cadre d'un instrument international une exception au principe de territorialité.

3.2 Accès transfrontalier aux données : dispositions pertinentes

3.2.1 Article 32

88 La question de savoir si un Etat et ses autorités peuvent avoir le droit, en vertu d'instruments nationaux ou internationaux, d'accéder unilatéralement à des données électroniques stockées à l'étranger est débattue depuis plus de vingt ans. Elle a été abordée lors des négociations sur la Convention de Budapest. Comme le note le Rapport explicatif concernant l'article 32, sur l'accès transfrontalier aux données :

> 293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des Etats agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret ; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. A cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.
>
> 294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations : d'abord, celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne « légalement autorisée » à communiquer des données peut varier en fonction des circonstances, de la nature de la personne et du droit applicable concernés. Par exemple, le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces

[47] C'est pourquoi le T-CY a décidé (en novembre 2011) d'évaluer la mise en œuvre par les Parties des articles sur la conservation rapide (16, 17, 29 et 30) et a proposé (en juin 2012) que le prochain cycle d'évaluations se concentre sur l'entraide judiciaire rapide (article 31).

personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article.

89 L'article 32 est donc la plus importante des dispositions sur l'accès transfrontalier prévues par la Convention. L'expérience de certains Etats parties montre que l'article 19.2, sur l'extension des perquisitions à des systèmes informatiques connectés au système initial, peut aussi présenter un intérêt. Enfin, la question de la compétence (article 22) appelle des discussions supplémentaires.

90 Il est important de retenir que selon le paragraphe 293 du Rapport explicatif,

- les Parties ont décidé de poursuivre la discussion et de réglementer des situations autres que celles prévues à l'article 32 ultérieurement, après avoir acquis davantage d'expérience ;

- les situations d'accès transfrontalier autres que celles figurant dans l'article 32 ne sont « ni autorisées ni exclues ».

3.2.2 Article 32a – Accès transfrontalier à des données publiques

91 L'article 32a couvre les situations dans lesquelles les données recherchées à l'étranger sont publiquement accessibles (données ouvertes) :

> Article 32 - Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public
>
> Une Partie peut, sans l'autorisation d'une autre Partie :
> a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; […]

92 Les enquêteurs sont autorisés à accéder directement à des données stockées qui ont été, par exemple, publiées sur un site Internet. Ils peuvent conserver ces données (en les téléchargeant, en effectuant des captures d'écran…) et les utiliser comme preuves dans une procédure pénale sans passer par l'entraide judiciaire et sans solliciter l'autorisation de l'Etat où se trouve le système informatique qui héberge le site.

93 L'article 32a autorise donc l'accès à des données qui peuvent être techniquement stockées à l'étranger. On peut considérer que cet accès à des données publiques à des fins de justice pénale est devenu une pratique internationalement reconnue et donc un élément du droit coutumier international, « étant donné qu'Internet est largement utilisé dans le monde entier, que les internautes ignorent souvent l'emplacement physique du stockage des données et que l'accès à des données publiques dans le cyberspace ne représente qu'un degré d'intrusion minime[48] ».

3.2.3 Article 32b – Accès transfrontalier avec consentement

94 L'article 32b couvre les situations où les autorités répressives d'un Etat accèdent à des données stockées à l'étranger avec l'accord exprès de la personne légalement autorisée à divulguer les données, sans avoir à en avertir les autorités de l'Etat concerné.

[48] Sieber (2012, page C144/145). Voir aussi Seitz (2004, page 9/10, sur http://www.ijclp.net/files/ijclp_web-doc_2-cy-2004.pdf).

> Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public
>
> Une Partie peut, sans l'autorisation d'une autre Partie :
> […]
> b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

95 Comme indiqué plus haut, l'article 32, et en particulier l'article 32b, est l'aboutissement de longues négociations. Les Etats parties n'ont pas réglementé ce point en détail, préférant une « ambiguïté constructive » permettant d'englober différentes situations. La Convention n'a délibérément pas exclu que les Parties aillent au-delà de l'article 32.

96 Plusieurs questions se sont posées concernant les éléments de l'article 32b.

3.2.3.1 Quel sens donner à « transfrontière » et à « situé » ?

97 D'après le paragraphe 293 du Rapport explicatif de la Convention de Budapest, l'accès transfrontière (ou transfrontalier) consiste à « accéder unilatéralement [c'est-à-dire sans passer par l'entraide judiciaire] aux données informatiques stockées sur le territoire d'une autre Partie ».

98 Cette mesure est applicable entre Parties à la Convention. Les Parties sont supposées se faire confiance et respecter, conformément à l'article 15, certains principes de droits de l'homme et de prééminence du droit.

99 L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat ». Il sous-entend que l'emplacement des données est connu.

100 L'article 32b, de même, ne couvre pas les situations dans lesquelles une personne donne son consentement alors que les données ne sont pas stockées dans un autre Etat Partie ou que leur emplacement est incertain.

101 Sachant que l'article « n'autorise ni n'exclut » d'autres situations, il appartient aux Etats, dans ces autres situations, d'évaluer la légitimité d'une perquisition ou d'un autre type d'accès à la lumière de son droit interne, des principes de droit international applicables ou de considérations liées aux relations internationales.

3.2.3.2 Qu'est-ce qu'un accès sans autorisation de l'autre Partie ?

102 Comme indiqué plus haut, il consiste à « accéder unilatéralement [c'est-à-dire sans passer par l'entraide judiciaire] aux données informatiques stockées sur le territoire d'une autre Partie ».

103 La Convention de Budapest ne demande pas que l'autre Partie soit avertie, au contraire du principe correspondant adopté par le G8 à Moscou en octobre 1999, qui suggérait d'« envisager d'avertir l'Etat perquisitionné ». La Convention de Budapest n'exclut pas non plus une telle notification. Les Parties peuvent avertir l'autre Partie concernée si elles le jugent utile.

3.2.3.3 Que faut-il pour que le consentement soit constitué ?

104 L'article 32b précise que le consentement doit être légal et volontaire, ce qui signifie que la personne qui autorise l'accès ou divulgue les données ne doit avoir été ni contrainte ni dupée[49]. Les éléments constitutifs du consentement sont régis par le droit interne de la Partie à qui le consentement est donné, en d'autres termes, de la Partie qui demande l'accès transfrontalier.

105 Selon certaines réglementations nationales, il se peut que le consentement ne puisse pas être donné par un mineur ou par des personnes se trouvant dans certaines situations (troubles mentaux par exemple).

106 Dans la plupart des Parties, la coopération dans le cadre d'une enquête pénale requiert un consentement exprès. Par exemple, le fait qu'une personne ait accepté les conditions d'utilisation générales d'un service en ligne ne constitue pas un consentement exprès, même si ces conditions indiquent que les données peuvent être transmises à des autorités judiciaires en cas d'abus.

3.2.3.4 **Quel droit s'applique ?**

107 L'article 32b ne précise pas quel droit s'applique pour définir le « consentement légal » et savoir si une personne est « légalement autorisée » à divulguer des données.

108 Dans les deux cas, pour des raisons pratiques, « légal » semble désigner le droit de la Partie qui perquisitionne. Lorsque l'accès transfrontalier revêt un caractère urgent, il ne semble pas réaliste que les autorités répressives qui perquisitionnent puissent vérifier les règles d'utilisation des données en vigueur dans l'autre Partie, et dans tous les cas, les autorités répressives agissent habituellement sur la base des lois de leur propre pays.

109 Cependant, s'il est évident que la divulgation des données ou l'autorisation d'y accéder violerait la législation de l'autre Partie ou sa réglementation sur l'utilisation des données, les autorités répressives devraient s'abstenir de poursuivre l'accès transfrontalier.

110 A cet égard, on peut concevoir que le droit interne interdise de divulguer à des autorités étrangères, sans en avertir les autorités nationales, des informations pouvant être utilisées dans des poursuites pénales. C'est le cas de la loi française dite « de blocage » (1980[50]) :

Article 1 bis (Créé par Loi 80-538 1980-07-16 art. 2 II JORF 17 juillet 1980)

---

[49] L'affaire Gorshkov/Ivanov de 2000 est souvent citée comme exemple d'application de l'article 32b, à tort, puisque les plaignants n'avaient pas volontairement consenti à l'accès. Dans tous les cas, la Convention de Budapest n'a été adoptée qu'en 2001, c'est-à-dire un an plus tard, et n'est entrée en vigueur qu'en 2004 ; les Etats-Unis y ont adhéré en 2006.
(Voir *United States v. Gorshkov*, n° CR00-550C, 2001 WL 1024026, *2 (W.D.Wash., 23 mai 2001), analysé dans http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf).

[50] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, version consolidée au 1er janvier 2002,
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000501326
Cette loi a été appliquée en 2007 dans une affaire de recherche de renseignements aux Etats-Unis. Un avocat français (« Christopher X »), agissant pour le compte de son client américain dans une procédure ouverte en Californie, avait sollicité des informations auprès d'un ressortissant français en France. Il a été mis en examen et condamné en vertu de l'article 1 de la « loi de blocage », arrêt confirmé par la Cour de Cassation.
http://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000017837490

> Sous réserve des traités ou accords internationaux et des lois et règlements en vigueur, il est interdit à toute personne de demander, de rechercher ou de communiquer, par écrit, oralement ou sous toute autre forme, des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci.

111 Cependant, cette disposition étant « sous réserve » des accords internationaux, la loi en question ne bloque pas la coopération en vertu de l'article 32b.

3.2.3.5 **Qui peut autoriser l'accès ou divulguer des données ?**

112 La personne légalement autorisée à divulguer des données peut varier en fonction des circonstances et des règles applicables. Le paragraphe 294 du Rapport explicatif offre un exemple simple, celui d'une personne autorisant l'accès à sa messagerie électronique ou à d'autres données qu'elle a stockées à l'étranger.

113 La personne qui autorise l'accès peut aussi être un prestataires de services via Internet ou en ligne ou toute autre entité privée détenant des données pour le compte d'un individu, par exemple, si les termes du contrat le permettent, si le prestataire de services est devenu propriétaire des données ou s'il a le pouvoir d'en disposer. Dans ce cas, pour se conformer à l'article 32b, le prestataire de services doit autoriser l'accès volontairement et légalement, c'est-à-dire entre autres sans porter atteinte à la vie privée ou à d'autres droits. Par conséquent, ce n'est généralement possible que pour les données dont l'entité privée est propriétaire, telles que les données de trafic, d'inscription ou de réseau, parfois sans qu'il ne soit possible de divulguer volontairement et légalement les contenus créés par les usagers. Dans ce cas, une injonction judiciaire de saisie ou de communication des données n'est pas couverte par l'article 32b[51].

3.2.3.6 **Où doit se trouver la personne qui fournit l'accès ou accepte de le fournir ?**

114 L'article 32b ne précise pas où doit se trouver la personne qui autorise l'accès au moment ou elle donne son accord et au moment où elle fournit effectivement l'accès.

115 Habituellement, la personne qui fournit l'accès se trouve physiquement sur le territoire de la Partie requérante. Dans ce cas, cette personne relève du ressort et des lois de l'Etat enquêteur[52]. C'était aussi l'hypothèse de travail du Comité PC-CY, chargé d'élaborer la Convention de Budapest[53]. Elle n'a pas été explicitée dans le texte définitif de la Convention.

---

[51] Pour différents scénarios, voir par exemple le rapport suivant, pp. 11-12 :
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

[52] Kaspersen, Henrik (2009) : « Cybercrime and internet jurisdiction » (analyse préparée pour le Conseil de l'Europe / Projet global sur la cybercriminalité), p. 27.
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

[53] Jusqu'à la version n° 19 (avril 2000), l'article 27 (précurseur de l'article 32) était assorti d'une note de bas de page :
« Ce paragraphe part du principe que l'Etat auteur de l'accès limitera ses contacts aux personnes se trouvant sur son territoire (bien que ces personnes puissent être appelées à contacter des personnes se trouvant sur d'autres territoires pour obtenir leur consentement ou une délégation de pouvoir). Cela pourrait être explicitement précisé, par l'insertion du texte entre parenthèses, ou faire l'objet de précisions dans le Rapport explicatif ».

116 Il y a en fait de multiples situations possibles. On peut imaginer que la personne physique ou morale se trouve sur le territoire des autorités répressives requérantes lorsqu'elle consent à divulguer les données ou lorsqu'elle y donne effectivement accès, ou uniquement lorsqu'elle consent mais non lorsqu'elle donne l'accès, ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle consent à divulguer les données et/ou y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle consent à coopérer ou lorsqu'elle fournit effectivement l'accès. S'il s'agit d'une personne morale (comme une entité privée), elle peut être représentée sur le territoire de l'autorité répressive requérante, sur le territoire où se trouvent les données, voire en même temps dans un pays tiers.

117 En 2009-2010, le T-CY a mené une première enquête sur la question de l'accès transfrontalier[54]. Les réponses au questionnaire reçues alors laissent penser que pour la plupart des Parties, le lieu où se trouve la personne fournissant l'accès n'a pas d'importance.

118 Cependant, la plupart des Parties (quoique non toutes) s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des autorités répressives étrangères recherchant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale.

3.2.4 Article 19.2 – Extension des recherches

119 L'article 19 est l'une des dispositions clés en matière de procédure. Il oblige les Parties à prévoir une législation permettant aux autorités compétentes de perquisitionner, de consulter, de saisir et de conserver des systèmes, données ou supports de stockage informatiques situés sur leur territoire. Les données informatiques, comme pour les éléments de preuve « traditionnels », doivent être rendues tangibles et utilisables aux fins de l'enquête et des poursuites pénales. Il appartient cependant aux Parties de veiller au respect des principes de la protection des données et du secret de la correspondance[55]. Un Etat peut par exemple considérer un e-mail stocké sur le serveur d'un prestataire de services comme une information en cours de communication[56] jusqu'à ce qu'il soit consulté ou téléchargé par l'usager ou le destinataire.

120 L'article 19.2 vise à permettre aux autorités répressives d'élargir rapidement une perquisition (ou d'autres types d'accès) aux systèmes informatiques légalement accessibles à partir du système initial lorsqu'elles ont des raisons de penser que les données recherchées peuvent être stockées dans cet autre système.

> Article 19 - Perquisition et saisie de données informatiques stockées
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :
> a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

[54] Dix-huit pays ont répondu au questionnaire (Allemagne, Bosnie-Herzégovine, Chili, Chypre, Etats-Unis d'Amérique, Finlande, Estonie, Hongrie, Japon, Lituanie, Moldova, Monténégro, Norvège, Portugal, Pologne, République tchèque, Suède et Turquie). Les réponses sont compilées dans le document T-CY(2010)01 et un projet d'analyse a été publié le 15 juin 2010 (T-CY(2010)05).

[55] Voir le paragraphe 190 du Rapport explicatif.

[56] Ce qui signifie que les autorités ne peuvent obtenir le contenu du message stocké qu'en appliquant leur pouvoir d'interception.

b à un support de stockage informatique permettant de stocker des données informatiques sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

121 Le Rapport explicatif souligne que l'article 19 renvoie à des mesures au niveau national et que le système auquel la recherche est étendue doit être situé sur le territoire des autorités qui effectuent cette recherche :

192. L'expression « sur son territoire » sert à rappeler que cette disposition, comme tous les articles de cette section, ne concerne que les seules mesures qui doivent être prises au niveau national.

193. Le paragraphe 2 habilite les autorités chargées d'une enquête à étendre l'opération entreprise pour perquisitionner ou accéder par un moyen similaire à un autre système informatique ou une partie de celui-ci lorsqu'elles ont des raisons de penser que les données sollicitées sont stockées dans cet autre système informatique.

194. La Convention ne prescrit pas les modalités d'autorisation ni d'application de l'extension de la mesure de perquisition. C'est à la législation interne qu'il appartient de les fixer. On peut citer quelques exemples d'options possibles : habiliter l'autorité, judiciaire ou autre, qui a autorisé la perquisition d'un système informatique donné à autoriser également l'extension de la perquisition ou du moyen d'accès similaire à un système connecté si elle a des raisons de penser (dans la mesure exigée par la législation nationale et les dispositions relatives à la défense des droits de l'homme) que le système informatique connecté pourrait contenir les données spécifiques recherchées ; habiliter les autorités chargées de l'enquête à étendre la perquisition ou l'accès par un moyen similaire autorisés d'un système informatique spécifique à un autre système informatique connecté lorsqu'il existe des raisons analogues de penser que les données spécifiques recherchées sont stockées dans l'autre système informatique ; ou exercer les pouvoirs de perquisition ou d'accès similaire aux deux endroits d'une façon coordonnée et rapide. Dans tous les cas de figure, les données à rechercher doivent être légalement accessibles à partir du système informatique initial ou disponible pour ce système initial.

195. Cet article ne traite pas des « perquisition et saisie transfrontières », qui donnent aux Etats une possibilité de perquisition ou un moyen d'accès similaire aux données se trouvant sur le territoire d'autres Etats sans avoir à recourir aux modalités habituelles de l'entraide judiciaire.

122 Bien que l'extension des recherches en vertu de l'article 19.2 soit conçue comme une mesure nationale, une question demeure : quelles règles s'appliquent lorsque les autorités répressives élargissent leur recherche à des systèmes informatiques situés à l'étranger sans en avoir conscience ou lorsqu'il est difficile de savoir sur quel territoire un système informatique est situé, et donc à qui il convient d'adresser les demandes d'assistance internationale ?

3.2.5 Article 22 – Compétence

3.2.5.1 **Principes généraux de la Convention de Budapest**

123 En matière de compétence, la Convention de Budapest établit les principes suivants :

> Article 22 – Compétence
>
> 1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :
> a sur son territoire ; ou
> b à bord d'un navire battant pavillon de cette Partie ; ou
> c à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou
> d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.
>
> 2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.
>
> 3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.
>
> 4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.
>
> 5 Lorsque plusieurs Parties revendiquent leur compétence à l'égard d'une infraction présumée établie conformément à la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

124 L'article 22 précise ainsi les critères à observer par les Parties lorsqu'elles poursuivent et sanctionnent des infractions pénales relevant des articles 2 à 11 de la Convention. Les alinéas b à d du paragraphe 1 reposent sur le principe du pavillon[57] et de la nationalité. Conformément au paragraphe 2, les Parties peuvent assortir ces dispositions de réserves.

125 Le paragraphe 1a, à caractère obligatoire, repose sur le principe de la territorialité. En vertu de la Convention, les Parties sont tenues d'établir leur compétence à l'égard des infractions qui sont commises sur leur territoire. S'agissant des infractions pénales « traditionnelles », le processus amenant à décider sur quel territoire l'infraction a été commise ne pose généralement pas de problème majeur.

126 La situation peut cependant s'avérer différente pour les infractions commises par des moyens électroniques ou visant un système informatique. S'agissant de données stockées informatiquement ou d'une personne agissant via des connexions en ligne, il est souvent difficile de savoir en quel lieu ou sur quel territoire un acte a été commis ou un effet s'est fait ressentir. Les choses se compliquent encore en cas d'utilisation de moyens technologiques comme

[57] Pour les navires et les aéronefs.

l'informatique décentralisée ou les périphériques externes. Lorsqu'un usager recourt à des services décentralisés, tout ou partie des données ne cessent de changer d'emplacement ou de serveur. Pour éviter les pertes de données et les rendre plus disponibles, elles peuvent être dupliquées. Pour les autorités et même pour le propriétaire des données, il peut devenir impossible de connaître l'emplacement actuel des données informatiques qui doivent être récupérées.

127 Comme indiqué plus haut, cette situation de « disparition du lieu », source de grande incertitude quant au lieu de stockage des données informatiques recherchées, représente un défi pour les Parties et pour les autorités répressives confrontées à la cybercriminalité.

3.2.5.2 **Application des règles de compétence[58]**

128 La première question de compétence à résoudre en matière d'accès transfrontalier est celle de la compétence à appliquer en vertu du principe de territorialité.

129 Les auteurs de la Recommandation R (95) 13 du Conseil de l'Europe[59] ont reconnu que les enquêtes transfrontalières étaient techniquement faisables et que les enquêteurs n'avaient pas toujours conscience que les systèmes et les données se trouvaient en territoire étranger, mais se sont accordés pour considérer

> que des activités d'enquête menées par les autorités répressives d'un Etat Partie sur des réseaux de communication internationaux ou sur des systèmes informatiques situés sur le territoire d'un autre Etat peuvent constituer une violation de la souveraineté territoriale de l'Etat concerné, et ne peuvent donc être entreprises sans le consentement préalable de cet Etat[60].

130 La règle de droit coutumier international considérée comme prédominante concernant la compétence à appliquer est aujourd'hui encore celle énoncée par la Cour permanente de justice internationale (CPJI) dans son arrêt sur l'affaire du « Lotus », en 1927 :

> la limitation primordiale qu'impose le droit international à l'Etat est celle d'exclure – sauf l'existence d'une règle permissive contraire – tout exercice de sa puissance sur le territoire d'un autre Etat. Dans ce sens, la juridiction est certainement territoriale ; elle ne pourrait être exercée hors du territoire, sinon en vertu d'une règle permissive découlant du droit international coutumier ou d'une convention[61].

131 Bien que soupçonnant qu'un accès transfrontalier via les TIC « puisse » porter atteinte à la souveraineté nationale et au principe de territorialité, les auteurs de la Recommandation R (95) 13 et les participants aux négociations sur la Convention de Budapest n'étaient pas certains qu'un tel accès, sans présence physique sur le territoire de l'autre Etat, constitue vraiment une atteinte au principe de territorialité au sens de l'arrêt « Lotus » de 1927. La solution adoptée dans la

---

[58] Pour une analyse des questions de compétence liées à la Convention de Budapest, voir http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

[59] Conseil de l'Europe / Comité des Ministres (1995) : Recommandation R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information ».

[60] Kaspersen, Henrik (2009) : « Cybercrime and internet jurisdiction » (analyse préparée pour le Conseil de l'Europe / Projet global sur la cybercriminalité), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

[61] Affaire du « Lotus » (France c. Turquie), CPIJ série A, n° 10, p. 18 (1927).

Convention de Budapest a consisté à n'autoriser l'accès transfrontalier que dans les conditions strictes énoncées à l'article 32[62].

132 Au sens de l'arrêt « Lotus », l'article 32 est donc « une règle permissive découlant du droit international coutumier ou d'une convention ».

133 Les auteurs de la Convention de Budapest ne considéraient pas l'article 32 comme une panacée, jugeant que les situations non prévues par cet article n'étaient « ni autorisées ni exclues » et que des solutions supplémentaires pouvaient être adoptées à une étape ultérieure[63].

134 Bien que le principe de territorialité reste prépondérant, la possibilité de l'appliquer dans le « cyberespace », fait de données voyageuses, fragmentées, composites ou dupliquées sur plusieurs serveurs relevant de divers ressorts territoriaux, suscite de plus en plus de doutes. Il n'est pas possible d'appliquer le principe de territorialité sans certitude quant à l'emplacement des données – d'où des appels à « changer de paradigme[64] ».

135 Pour débattre de « règles permissives » supplémentaires et de nouvelles exceptions au principe de territorialité, comme l'accès transfrontalier sans consentement, les questions suivantes pourraient stimuler la réflexion et aider à préciser le principe de territorialité :

- L'accès transfrontalier revient-il vraiment à exercer un pouvoir « sur » un territoire étranger, si les enquêteurs accèdent aux données depuis leur propre territoire[65] ?
- Quel est le lien entre les données et le territoire sur lequel elles sont stockées ? Par exemple, dans quelle mesure le principe de territorialité s'applique-t-il en cas d'accès transfrontalier
  - si la personne habilitée à disposer des données est physiquement présente sur le territoire des autorités enquêtrices tandis que les données sont stockées dans un autre Etat ?
  - si les adresses IP liées à une communication faisant l'objet d'une enquête relèvent du territoire des autorités enquêtrices alors que les données elles-mêmes sont stockées dans un autre Etat ?
- Comment appliquer le principe de territorialité
  - lorsqu'on ignore dans quel Etat les données consultées sont physiquement stockées ?
  - si différentes copies des données sont stockées dans des Etats différents ?
  - si les données « voyagent » d'un pays à un autre ?

---

[62] Nous reviendrons plus en détail sur l'article 32 plus loin dans ce rapport.

[63] Rapport explicatif de la Convention de Budapest, paragraphe 293.

[64] Discussions lors de la Conférence Octopus 2012 (www.coe.int/octopus2012). Voir aussi Salt, Marcos (2012) : « Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina » (contribution à la Conférence Octopus du Conseil de l'Europe, 2012).

[65] D'une part, l'accès à des données informatiques n'est pas un acte répressif *concret*, comparable par exemple à la saisie de matériel. Cependant, en droit international, l'exercice de pouvoirs étatiques ne passe pas nécessairement par des moyens *matériels / tangibles.* Concernant l'immunité par exemple, la Cour internationale de justice (CIJ) a considéré dans l'affaire « du mandat d'arrêt » : « l'*émission* du mandat d'arrêt […], comme telle, constitue un acte de l'autorité judicaire ». (Affaire relative au mandat d'arrêt du 11avril 2000 (*République démocratique du Congo c. Belgique*), arrêt, *Recueil CIJ* 2002, paragraphe 70). Voir aussi l'opinion individuelle commune des juges Higgins, Kooijmans et Buergenthal : « La délivrance d'un mandat d'arrêt international […] est analogue au verrouillage d'un radar sur un aéronef : c'est déjà une déclaration de la volonté et de la capacité d'agir et, en tant que telle, elle peut être perçue comme une menace de le faire » (Opinion individuelle commune, paragraphe 69).

- si les données sont fragmentées et réparties entre plusieurs Etats, ou composées de sources venant de plusieurs Etats différents ?

- Dans quelle mesure les autorités enquêtrices interviennent-elles dans les affaires intérieures de l'Etat où se trouvent les données ?
- Quel impact a l'accès transfrontalier sur les intérêts de l'Etat où se trouvent les données ?
- Quel impact a l'accès transfrontalier sur les droits des suspects ? La législation de l'Etat enquêteur sur la protection de la vie privée et des droits procéduraux des personnes dont les données sont consultées fait-elle une différence ?
- Y a-t-il une différence si l'accès aux données par des autorités répressives a été ordonné légalement par le pays de ces autorités et fait l'objet de conditions et de garanties telles que celles prévues à l'article 15 de la Convention de Budapest ?
- La nature des données obtenues à l'étranger (données de trafic, d'inscription ou de contenu) fait-elle une différence ?
- Quel impact a l'accès transfrontalier sur les intérêts de tierces parties ?
- Quel est l'intensité ou le degré d'intrusivité de la mesure transfrontalière ? Y a-t-il une différence si les autorités répressives consultent des données publiques, conservent une copie de données non publiques ou interviennent dans des données (modification, suppression…) ou dans un système (désactivation, blocage, entrave au fonctionnement) situés dans un autre Etat ? Y a-t-il une différence si les autorités répressives accèdent aux données via un mot de passe ou d'autres moyens obtenus légalement ou si elles doivent les pirater ?
- L'accès transfrontalier devrait-il être permis même sans consentement dans les situations urgentes ? Le fait que l'enquête porte sur un crime grave ou qu'il existe un risque immédiat pour la vie ou l'intégrité physique fait-il une différence ?
- Dans quelle mesure des critères tels que la réciprocité ou la double incrimination s'appliquent-ils ?

4 Scénarios d'accès transfrontalier

136 Le présent chapitre résume les résultats de l'enquête menée en 2009-2010 par le T-CY, les pratiques signalées par les Etats et les informations disponibles sur l'accès transfrontalier via des prestataires de services ou d'autres entités privées.

4.1 Accès direct des autorités répressives aux données : pratiques signalées en 2009-2010

137 Le T-CY a mené en 2009-2010 une enquête sur l'accès transfrontalier direct aux données et flux de données. Les réponses indiquent que beaucoup d'autorités répressives nationales effectuent des perquisitions transfrontalières mais que les conditions et les pratiques diffèrent. Dans de nombreux cas, les pratiques ont encore évolué depuis l'enquête. Il est à souligner que cette analyse ne porte pas sur toutes les Parties à la Convention[66]. Les questions portaient sur cinq scénarios possibles.

4.1.1 Scénario A – Accès transfrontalier lors d'une perquisition de locaux

> Lors d'une perquisition dans les locaux d'un suspect, vos forces de l'ordre trouvent un ordinateur encore allumé. Elles obtiennent légalement du suspect arrêté le mot de passe permettant d'accéder à des données stockées dans un autre système informatique présentant un contenu présumé illégal ou d'autres preuves à charge appartenant au suspect.

138 Dans la plupart des Etats ayant répondu[67], les autorités répressives peuvent directement accéder aux données disponibles à partir de l'ordinateur du suspect, du moment que le ressort territorial des données n'est pas évident. La plupart peuvent aussi accéder à des données à partir de l'ordinateur du suspect en utilisant son mot de passe.

139 S'il est clair que des données informatiques sont stockées à l'étranger, les autorités répressives peuvent toujours accéder aux données dans sept pays[68] mais n'y ont plus droit dans dix pays[69], à moins que le suspect ne coopère volontairement comme prévu à l'article 32b. Cela s'applique aussi à l'accès au moyen du mot de passe du suspect.

140 Dans neuf Etats, les données ainsi obtenues peuvent être utilisées dans une procédure pénale même si la procédure ne repose pas sur une autorisation spécifique en droit international, comme l'article 32b de la Convention de Budapest[70]. Dans les autres Etats ayant répondu, cela dépend des circonstances précises.

---

[66] Dix-huit pays ont répondu au questionnaire (Allemagne, Bosnie-Herzégovine, Chili, Chypre, Etats-Unis d'Amérique, Finlande, Estonie, Hongrie, Japon, Lituanie, Moldova, Monténégro, Norvège, Portugal, Pologne, République tchèque, Suède et Turquie). Les réponses sont compilées dans le document T-CY(2010)01 et un projet d'analyse a été publié le 15 juin 2010 (T-CY(2010)05).

[67] Finlande, Lituanie, Portugal, Pologne, Suède, Turquie, Chili, Bosnie-Herzégovine, Monténégro, Chypre, Japon, Hongrie, Etats-Unis. Pour la République tchèque, l'Estonie et l'Allemagne, la réponse dépend des circonstances précises de la perquisition.

[68] Finlande, Portugal, Pologne, Chili, Monténégro, Japon, Etats-Unis.

[69] République tchèque, Lituanie, Allemagne, Suède, Turquie, Bosnie-Herzégovine, Japon, Hongrie, Estonie et Pays-Bas. A Chypre, cela dépend du type de données ; pour les réseaux sociaux, l'accès est autorisé.

[70] Finlande, Norvège, Portugal, Pologne, Suède, Turquie, Japon, Chili, Estonie (si le suspect coopère).

141 Dans presque tous les pays, l'urgence ou le risque de perte de preuves ne changent rien à l'autorisation ou non de l'accès transfrontalier selon le scénario ci-dessus.

142 Dans certains Etats, les autorités étrangères doivent être averties[71] ; dans d'autres, ce n'est pas nécessaire[72] ou cela dépend des circonstances précises.

4.1.2 Scénario B – Accès transfrontalier via un mot de passe obtenu légalement

> Vos forces de l'ordre ont obtenu, par des moyens légaux, un mot de passe permettant d'accéder à des données informatiques susceptibles de comporter un contenu illégal ou des preuves à charge.

143 Les autorités répressives de presque tous les pays ayant répondu au questionnaire peuvent accéder aux données depuis leurs propres systèmes informatiques si le territoire sur lequel les données sont stockées n'est pas évident.

144 S'il est clair que les données sont stockées à l'étranger, les autorités répressives de la plupart des pays peuvent toujours accéder aux données depuis leur propre système informatique[73].

145 Comme dans le scénario précédent, dans la plupart des Etats, les données ainsi obtenues peuvent être utilisées dans une procédure pénale même si la procédure ne repose pas sur une autorisation spécifique en droit international, comme l'article 32b de la Convention de Budapest[74]. Dans les autres Etats ayant répondu, cela dépend des circonstances précises.

146 Là encore, dans presque tous les Etats, l'urgence ou le risque de perte de preuves ne changent rien à l'autorisation ou non de l'accès transfrontalier selon ce scénario.

147 Dans certains Etats également, les autorités étrangères doivent être averties tandis que dans d'autres, ce n'est pas nécessaire ou cela dépend des circonstances précises.

4.1.3 Scénario C – Accès transfrontalier via des logiciels ou moyens techniques spéciaux

> Au cours d'une enquête pénale, vos forces de l'ordre ont appris l'existence d'un système informatique susceptible de comporter des contenus illégaux ou d'autres preuves à charge.

148 Les autorités répressives de certains Etats ont le droit d'accéder à distance à des données via des logiciels spéciaux (enregistreurs de frappe, programmes renifleurs) ou d'autres moyens techniques si le ressort territorial dont relève le système n'est pas évident. Cependant, la majorité des Etats n'autorisent pas une telle démarche ou la soumettent à des conditions très strictes.

149 S'il est clair que le système informatique relève d'une compétence étrangère, presque tous les Etats ayant répondu interdisent ce type de mesure[75].

150 Dans presque tous les Etats, la question de savoir si les preuves ainsi obtenues peuvent être utilisées dans une procédure pénale n'est pas clairement tranchée.

---

[71] République tchèque, Portugal, Pologne, Chili, Bosnie-Herzégovine, Monténégro.

[72] Lituanie, Suède, Turquie.

[73] Il y a des exceptions : République tchèque, Lituanie, Suède, Hongrie, Estonie et Pays-Bas.

[74] Finlande, Norvège, Portugal, Pologne, Suède, Turquie, Japon, Chili, Estonie.

[75] Exceptions : Bosnie-Herzégovine, Japon et éventuellement Chili.

4.1.4 Scénario D – Accès transfrontalier avec consentement (article 32b)

> Au cours d'une enquête pénale, une personne a légalement et volontairement autorisé vos forces de l'ordre à accéder à des données informatiques stockées à l'étranger et qui pourraient constituer des preuves importantes.

151 En pareil cas, les autorités répressives de presque tous les Etats peuvent consulter et établir (c'est-à-dire télécharger) des données si la personne fournissant l'accès se trouve physiquement sur leur territoire.

152 Si la personne qui fournit l'accès se trouve physiquement dans l'Etat où sont stockées les données, ces actions restent possibles pour les autorités répressives de la plupart des Etats[76] ; dans d'autres, elles sont exclues, à la limite de la légalité, soumises à des conditions supplémentaires ou non clairement réglementées.

153 Dans la plupart des Etats[77], il est pertinent de savoir si la personne qui fournit l'accès est autorisée à divulguer les données conformément aux lois du territoire où sont stockées les données. Dans seulement deux Etats ayant répondu[78], les autorités répressives doivent en avertir l'autre Etat. Lorsque les autorités répressives ignorent où se trouvent les données, les Etats peuvent toujours agir, de bonne foi.

154 Dans la plupart des Etats ayant répondu, les preuves ainsi obtenues peuvent être utilisées dans une procédure pénale, même sans reposer sur une règle permissive en vertu du droit international (comme l'article 32b) ou sur une demande d'entraide judiciaire.

4.1.5 Scénario E – Informations fournies par un prestataire de services[79]

> Dans le cadre d'une enquête pénale, vos forces de l'ordre doivent obtenir des informations techniques concernant un suspect auprès d'un prestataire de services Internet.

155 Dans tous les Etats ayant répondu, les prestataires de services sont tenus de transmettre des informations techniques aux autorités répressives lorsque les données concernent un ressortissant national et sont situées et gérées sur le même territoire que celui des autorités en question.

156 Si les données concernent un ressortissant du pays des autorités répressives mais sont situées et gérées à l'étranger, la plupart des autorités doivent formuler une demande d'entraide. Il en va de même si les données concernent un étranger ayant commis une infraction sur le territoire des autorités répressives concernées, mais sont stockées et gérées dans un autre Etat.

157 Dans la plupart des Etats, les autorités répressives rencontrent des difficultés techniques et juridiques lorsqu'elles souhaitent obtenir des données stockées et gérées dans un autre Etat.

---

[76] République tchèque, Finlande, Portugal, Pologne, Suède, Japon, Chili, Bosnie-Herzégovine, Hongrie, Estonie, Etats-Unis.

[77] République tchèque, Finlande, Portugal, Pologne, Suède, Chili, Monténégro, Hongrie, Etats-Unis. Aspect non pertinent : Bosnie-Herzégovine, Chypre, Japon et Lituanie.

[78] Bosnie-Herzégovine et Pologne. Dans d'autres Etats cependant, ce point est traité au cas par cas.

[79] Note : ces informations ont été fournies en 2009. Il semble cependant qu'entre-temps, certains prestataires transnationaux aient revu leur politique et soient désormais prêts à divulguer des données d'inscription et de trafic à des autorités répressives nationales, sous certaines conditions et sur réception d'une demande légale, même si les données sont stockées sur un autre territoire.

158 Dans certains Etats, les prestataires de services peuvent répondre directement à des demandes émanant d'autorités répressives étrangères.

4.2 Accès direct des autorités répressives aux données : exemples nationaux

159 Dans de nombreux Etats de différentes régions du monde, il semble que les autorités répressives accèdent à des données relevant d'un autre ressort territorial dans le cadre d'enquêtes pénales nationales[80]. Cependant, les exemples à ce sujet sont rares. Les informations qui suivent ont été fournies au Groupe sur l'accès transfrontalier par certaines des Parties.

4.2.1 Belgique[81]

160 Conformément à la théorie dite « de l'ubiquité objective », une infraction est rattachée à tous les territoires où se situe au moins l'un de ses éléments matériels. Cette théorie est associée à celle « de l'indivisibilité », selon laquelle un tribunal peut se déclarer compétent pour tous les éléments liés à l'infraction. La Belgique applique en effet une combinaison de différents principes en matière de compétence (lieu de commission de l'infraction, instrument utilisé et effets directs).

161 Concernant l'exécution de la loi, c'est-à-dire la perquisition de systèmes informatiques, une solution spécifique a été adoptée en 2000, à savoir l'article 88ter du Code d'instruction criminelle belge (ci-après : « le Code »).

162 Le 28 novembre 2000, un an avant l'ouverture à la signature de la Convention de Budapest sur la cybercriminalité, le législateur belge a adopté la loi relative à la criminalité informatique, qui a ajouté au Code d'instruction criminelle l'article 88ter. Cette disposition correspond aux articles 19.2 et 32 de la Convention de Budapest.

163 L'article 88ter du Code autorise le juge d'instruction (c'est-à-dire le juge spécifiquement chargé de mener l'enquête et doté de pouvoirs d'enquête spéciaux), lorsqu'il ordonne une recherche dans un système informatique, à étendre cette recherche à tout ou partie d'un système informatique se trouvant dans un autre lieu.

164 Cette compétence est assortie de conditions. Le juge d'instruction ne peut prendre cette décision que :

(1) si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction, et

(2) (i) si d'autres mesures seraient disproportionnées (il faudrait par exemple émettre différents ordres de perquisitions pour différents locaux), ou

[80] Par exemple, il semble que les autorités répressives de nombreux pays d'Amérique latine accèdent à des données stockées dans des systèmes informatiques étrangers depuis un ordinateur, situé dans leur pays, depuis lequel elles sont légalement autorisées à effectuer une telle action. Elles le font habituellement avec l'accord de la personne habilitée à divulguer les données, à travers la coopération volontaire d'entités privées ou au moyen de mots de passe ou de codes d'accès obtenus légalement (sans recours au piratage). Voir Salt, Marcos (2012), « Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina » (contribution à la Conférence Octopus 2012 du Conseil de l'Europe).

[81] Résumé d'une contribution de Jan Kerkhofs (procureur) et de Philippe Van Linthout (juge d'instruction), Belgique, avril 2012.

(ii) s'il existe un risque que sans cette extension, des éléments de preuve soient perdus (condition presque toujours remplie dans les affaires de cybercriminalité, compte tenu de l'évanescence des preuves numériques).

165 Le législateur ne souhaitant pas permettre à la police d'aller trop facilement trop loin (par exemple, du compte bancaire d'un suspect à tous les comptes bancaires du même établissement), une autre condition a été ajoutée : le juge d'instruction doit limiter l'extension de la recherche aux systèmes informatiques ou parties de ces systèmes auxquels les utilisateurs du système initial ont accès (le plus souvent, le juge d'instruction autorise la police à entrer dans un autre système en utilisant l'identifiant et le mot de passe du suspect, qui délimitent le champ d'extension de la recherche).

166 A l'issue de la recherche étendue, le juge d'instruction doit en informer le responsable du système informatique, à condition qu'il puisse être raisonnablement identifié (la plupart du temps, ce n'est pas le cas).

167 La partie la plus novatrice de l'article 88ter du Code réside dans le dernier alinéa du paragraphe 3, qui prévoit que lorsque les données recueillies ne se trouvent pas sur le territoire belge, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction en informe simplement le ministère de la Justice, par l'intermédiaire du ministère public ; le ministère de la Justice en informe à son tour l'Etat concerné, s'il peut être raisonnablement déterminé (ce qui est rarement le cas).

168 Conformément à l'article 39bis du Code d'instruction criminelle, les données copiées peuvent être utilisées devant un tribunal au même titre que les données originales (elles ne sont pas physiquement saisies, mais néanmoins considérées comme telles).

169 Cela signifie, par exemple, que la police belge peut recueillir des preuves à partir d'ordinateurs situées en Belgique (pas nécessairement l'ordinateur du suspect) et de là, se rendre sur des serveurs situés dans n'importe quel pays. Elle peut examiner un compte à partir du moment où elle en possède l'identifiant et le mot de passe.

170 C'est clairement un avantage, permettant de gagner un temps précieux et de ne pas laisser perdre des preuves numériques à cause de formalités trop lourdes.

171 Il faut cependant souligner que malgré l'énorme potentiel que semble avoir l'article 88ter, le travail de police classique reste tout aussi important. En l'absence d'identifiants ou de mots de passe, découverts par exemple à l'aide d'un dispositif d'enregistrement classique, un compte de messagerie électronique reste inaccessible. Il faudrait pour cela que la loi offre la possibilité de le pirater.

172 Dans tous les cas, la solution adoptée par la Belgique offre de nombreuses possibilités de traitement de données stockées en ligne. Les entreprises et particuliers conservent en ligne non seulement des données, mais aussi des systèmes de traitement, si bien qu'ils ignorent où les données sont stockées exactement. La solution retenue en Belgique précise bien que l'important n'est pas de savoir *où* les données sont stockées, mais *à partir d'où* elles sont accessibles.

4.2.2 Pays-Bas

4.2.2.1 **Situation juridique aux Pays-Bas**

173 S'agissant des recherches à des fins d'enquête, les dispositions les plus pertinentes sont les articles 125 i, j et o et 126 l du Code de procédure pénale néerlandais (ci-après : « le Code »). Rédigées

en réponse à la Convention de Budapest, elles sont entrées en vigueur en 2006. Les articles 125 j et 126 l sont particulièrement importants. L'article 125 j prévoit qu'au cours d'une perquisition (d'un domicile ou de locaux[82]), il est possible, lorsque l'ordre de perquisition le permet, de fouiller les ordinateurs présents sur les lieux. Les recherches doivent être faites sur place. Les recherches en ligne et la poursuite des recherches sont aussi autorisées (dans certaines limites) du moment que le propriétaire légitime donne son accord. Autrement, le juge d'instruction peut ordonner la communication des mots de passe (sauf au suspect, qui n'est pas obligé de s'auto-incriminer). Cependant, l'article 126 l permet, sous certaines conditions, d'enregistrer des informations confidentielles « communiquées » via un ordinateur relié à un réseau. Ce pouvoir ne peut clairement pas être utilisé pour détecter des informations « stockées ». Par conséquent, et concrètement, ce pouvoir d'enquête n'est pas réputé utilisable, par exemple, pour obtenir un mot de passe nécessaire à l'accès à des informations codées.

174 Concernant l'extension des recherches aux systèmes hors des Pays-Bas, la note explicative de la loi néerlandaise sur la cybercriminalité prévoit expressément qu'elle n'est « pas autorisée » ; ce ne peut être fait que par le biais du droit international public. Dans la pratique, cela signifie que les autorités répressives doivent recourir à l'entraide judiciaire.

175 L'article 24 de la loi sur la sécurité et les services de renseignement prévoit des pouvoirs beaucoup plus larges concernant l'accès à un ordinateur pour y récupérer des informations stockées[83]. Cependant, les informations recueillies par ces moyens ne peuvent être utilisées dans une procédure pénale. Rien n'est dit quant à la possibilité de mener ces recherches de façon transfrontalière.

4.2.2.2 **Nécessité d'améliorer les enquêtes. Point de vue de la police et du parquet néerlandais**

176 Aux Pays-Bas, les enquêtes sur les infractions pénales sont confiées à un procureur. Afin d'accélérer et de rendre plus efficaces les enquêtes sur la cybercriminalité, le parquet néerlandais a demandé, à la fois dans les médias et à travers ses contacts réguliers avec le ministère de la Sécurité et de la Justice, des pouvoirs d'enquête plus larges et applicables de façon transfrontalière.

177 Il y a plusieurs raisons à cette demande. Le parquet et la police observent les tendances générales du numérique dans la société. De plus en plus de données sont stockées, traitées, transférées. Différents matériels informatiques sont utilisés simultanément ou successivement par la même personne (PC, réseau, ordinateur portable avec Wifi et autres outils mobiles comme les tablettes et les smartphones). Les services en ligne, donc décentralisés, rencontrent un succès de plus en plus grand. De plus en plus de citoyens innocents voient leurs ordinateurs détournés par des logiciels malveillants pour participer à des attaques massives qui menacent à la fois les internautes, les entreprises et les infrastructures nationales. Les usagers d'ordinateurs, y compris les cybercriminels, ont appris à encoder leurs données et sont passés maîtres dans l'art de se faire anonyme sur Internet (navigation anonyme via des adresses IP étrangères, serveurs proxy, routeur TOR (pour « The Onion Routeur »). Il est de plus en plus difficile de mettre la main sur des données utilisables comme preuves ou comme « pistes » pour une enquête. Cela vaut aussi

[82] Les perquisitions ne sont autorisées que pour certains crimes graves (sanctionnés par d'importantes peines maximales de prison).

[83] L'article 24, entre autres dispositions, énonce que « les services peuvent accéder à un ordinateur en usant de moyens techniques, de faux messages ou de fausses clés, ou en demandant à un agent de jouer le rôle d'une autre personne ». Les services de renseignement sont autorisés à pénétrer par infraction dans tout système sécurisé, par exemple en utilisant des moyens techniques pour intercepter des mots de passe et accéder à des informations codées.

bien pour les cybercriminels « nationaux », qui visent des victimes aux Pays-Bas ou à l'étranger en utilisant des IP étrangères, des serveurs proxy ou le routeur TOR, que pour les cybercriminels « étrangers » qui visent des victimes aux Pays-Bas ou utilisent les infrastructures technologiques néerlandaises. La cybercriminalité est par nature sans frontières.

178 Les procureurs et la police ont besoin d'accéder aux données suivantes :

- données de contenu :
  - par exemple, une collection d'images d'enfants abusés dissimulée ou stockée sur un ordinateur ou un périphérique, éventuellement codé ;
  - une collection de mots de passe, des informations sur des comptes bancaires personnels obtenus par piratage ou par hameçonnage ;
  - des plans de sabotage (par exemple) enregistrés dans un programme informatique (MS ou Apple) ;
  - une comptabilité falsifiée à l'aide d'un logiciel ;

- données de trafic :
  - utilisation de nouvelles techniques de messagerie (par blackberry par exemple) au lieu de l'envoi de textos ou d'appels depuis un téléphone portable ;
  - données téléchargées en ligne.

179 Le parquet néerlandais a lancé des propositions de réformes, comme le pouvoir de mener des « perquisitions en ligne » et de « contre-pirater » les systèmes informatiques utilisés pour des actes de cybercriminalité (attaque par saturation, piratage, infection par des virus). Ces techniques engloberaient le contrôle d'ordinateurs à distance, pour y installer des enregistreurs de frappe, pour consulter des données ou même pour les copier à l'insu de leur propriétaire. Les médias et les universitaires mentionnent également l'usage de logiciels espions par la police (du type du logiciel allemand « Bundestrojaner »). Le parquet néerlandais insiste sur le fait qu'une telle réforme législative nationale ne sera efficace que si l'usage transfrontalier de ces pouvoirs fait l'objet d'un accord international.

180 En pratique (voir plus loin), dans le cadre de plusieurs opérations, la police et le parquet néerlandais ont tenté de mener des enquêtes transfrontalières innovantes au sein du cadre juridique existant. Ils n'en continuent pas moins à demander l'amélioration du cadre national et international.

4.2.2.3 **Exemple pratique : l'affaire Bredolab**

181 L'affaire Bredolab, conclue en 2010, a abouti au démantèlement d'un vaste réseau zombie qui utilisait au moins 143 serveurs hébergés par un prestataire néerlandais. Ses origines et la plupart des machines utilisées étaient cependant étrangères. Ce réseau zombie avait infecté plus de 30 millions d'ordinateurs. Le côté exceptionnel de cette affaire réside dans le fait que les autorités répressives néerlandaises ont pris contrôle du réseau et envoyé un message écrit à tous les ordinateurs concernés pour signaler qu'ils étaient infectés par ce réseau, avant de fermer les serveurs utilisés par le réseau. Même si le magistrat avait donné son accord, il n'est pas certain que cette action était autorisée par le droit national, le message envoyé par la police néerlandaise pouvant être considéré comme un accès illégal à un ordinateur.

4.2.2.4 **Exemple pratique : l'affaire Descartes**

182 Dans l'affaire Descartes, une affaire de pédopornographie toujours en cours, le magistrat a autorisé la perquisition de serveurs TOR (« The Onion Router ») dont on savait qu'ils ne se

trouvaient pas aux Pays-Bas (mais probablement aux Etats-Unis). Ces serveurs comportaient de très violentes images d'enfants abusés. Via un formulaire en ligne, il était même possible de « commander » un viol d'enfant et d'enregistrer les images de la scène. Des copies numériques des informations à charge ont été effectuées au cours de la perquisition et de la saisie des serveurs TOR, en vue de la procédure pénale, et les données figurant sur le serveur ont été détruites. En outre, conformément à la loi néerlandaise (article 125 du Code de procédure pénale), le serveur a été bloqué de manière à empêcher l'accès aux données, puisqu'il constituait un crime aux Pays-Bas (article 240 b du Code de procédure pénale sur la pédopornographie).

183 Cette enquête comporte deux risques susceptibles d'entrer dans le champ de l'article 32b de la Convention de Budapest. Il peut y avoir atteinte à la souveraineté d'autres pays, et les données figurant sur les serveurs – qui constituent un crime en droit néerlandais – ont été rendues inaccessibles.

184 Sur la question de la souveraineté, les autorités répressives néerlandaises ont cherché à travailler en étroite coopération avec les Etats-Unis, supposant que les serveurs contenant les données incriminées se trouvaient dans ce pays. Les informations copiées ont été partagées avec les autorités répressives étasuniennes.

185 S'agissant des données rendues inaccessibles, cette opération a été approuvée au préalable par un juge néerlandais. En outre, les internautes cherchant à accéder aux informations – sans succès – étaient avertis, par un message des autorités répressives néerlandaises, que les données qu'ils cherchaient à consulter constituaient un crime aux Pays-Bas et avaient par conséquent été rendues inaccessibles.

4.2.2.5 Exemple pratique : lecture de messages électroniques hébergés par un prestataire étranger

186 Dans cette affaire de 2009, un procureur néerlandais a adressé une injonction de produire à un prestataire de services étranger en demandant des e-mails liés à un compte de messagerie spécifique. Un « informateur » avait transmis au procureur le nom d'utilisateur, l'identifiant et le mot de passe d'une messagerie électronique où des e-mails contenaient des informations sur un trafic de stupéfiants vers les Pays-Bas. Apparemment, le prestataire concerné a trop tardé à répondre et le procureur a demandé à la police d'accéder à la messagerie via un logiciel. Les messages recueillis ont permis de déduire que la drogue devait arriver au port de Rotterdam. Un suspect néerlandais a été arrêté. Au cours de son procès, le tribunal (de première instance) a jugé que la police n'était pas autorisée à consulter la messagerie sans l'accord de son propriétaire légitime. Il a également jugé que l'exécution extraterritoriale de ce pouvoir n'était pas non plus autorisée. Cette décision a été cassée en deuxième instance au motif que les droits du suspect n'avaient pas été violés, le compte de messagerie ne lui appartenant pas. La juridiction de deuxième instance est donc revenue sur la réduction de peine qui avait été accordée au suspect. On pourrait avancer que l'accès à son compte de messagerie a été considéré comme justifié.

4.2.2.6 Point de vue néerlandais sur l'encadrement des pouvoirs d'enquête dans le monde numérique

187 Le ministère de la Sécurité et de la Justice souscrit à une décision parlementaire intitulée *Motie Franken*. Cette décision précise les critères à remplir pour qu'une atteinte à la vie privée soit justifiée :

- Nécessité, efficacité et faisabilité de la mesure
- Proportionnalité avec l'infraction

- Evaluation préalable des risques présentés par une telle mesure
- Contrôle approprié et indépendant de la mesure.

188 Les professionnels du droit néerlandais utilisent des critères supplémentaires, comme par exemple :

- Mesure prévue par la loi
- Approbation préalable par un magistrat
- Transparence, la Partie / l'Etat concerné étant averti au plus tôt
- Transparence, les autorités répressives gardant trace de toutes leurs actions.

4.2.3 Norvège

189 La loi norvégienne de 1981 sur la procédure pénale définit quand et comment les autorités répressives peuvent accéder à des preuves, y compris les preuves électroniques. Les dispositions sont générales et les preuves électroniques ne sont pas réglementées en tant que telles, mis à part quelques dispositions spécifiques de la loi sur les communications électroniques (article 2-9), qui permettent aux autorités répressives d'obtenir des renseignements sur la clientèle directement auprès d'un prestataire de services, sans mandat judiciaire.

190 Il n'existe pas à ce jour de jurisprudence norvégienne sur l'usage des données recueillies par accès transfrontalier comme preuves dans une procédure pénale.

191 D'après la doctrine juridique norvégienne[84], les autorités répressives norvégiennes peuvent accéder à des données stockées électroniquement de la même façon que le propriétaire du compte pourrait le faire légalement, du moment qu'un ordre de perquisition a été émis et à condition que l'identifiant et les codes d'accès nécessaires soient disponibles.

192 Il n'existe pas de statistiques sur la fréquence de telles interventions. L'expérience montre que l'accès à des données stockées dans d'autres pays concerne habituellement les e-mails et les médias sociaux et repose sur le consentement du suspect, en accord avec l'article 32 de la Convention de Budapest.

193 Dans des situations plus rares, les recherches portent sur des données non protégées, le plus souvent disponibles via un smartphone. De telles enquêtes peuvent être lancées à l'initiative de la police, face à des activités suspectes. Il y a quelques années, les données en question n'auraient été stockées que sur le téléphone. Aujourd'hui, de plus en plus de données sont stockées via des applications décentralisées et « toujours disponibles ». Dans quelques cas, une perquisition permet de trouver un papier sur lequel le suspect a noté son identifiant et son mot de passe.

194 Dans une affaire, la police avait demandé la perquisition de la succursale norvégienne d'une entreprise active entre autres en Norvège. Au cours de la perquisition, on découvrit que l'entreprise ne stockait aucune donnée en Norvège ; tous les dossiers de l'entreprise étaient conservés dans un Etat tiers et consultés via des terminaux légers. A l'arrivée de la police, les ordinateurs étaient allumés. En raison de contraintes techniques, il n'a pas été possible de mettre la main sur les données en question (mis à part quelques sorties papier), mais selon la doctrine juridique norvégienne, il aurait été légal d'accéder à ces données et de les conserver et elles auraient ensuite pu être utilisées comme preuves dans la procédure pénale.

[84] *Lov og rett i cyberspace*, Inger Marie Sunde, 2006, p. 274

195 Dans d'autres affaires, les recherches sont fondées sur des demandes de conservation rapide suivies de demandes d'entraide judiciaire, par exemple pour obtenir des données de contenu à partir de réseaux sociaux ou de fournisseurs de messagerie. Dans une affaire, des tiers anonymes ont pénétré dans l'un des comptes de messagerie d'un suspect, ont sauvegardé tous les e-mails disponibles et les ont transmis à la police. La police ne les a pas utilisés comme preuves mais a adressé une demande d'entraide judiciaire à la police de l'Etat où se trouvait le siège du prestataire de messagerie afin de récupérer les e-mails et les données associées. Dans cette affaire, il était clair que ces messages allaient être utilisés comme preuves et non simplement comme sources d'informations. De toute évidence, il était également nécessaire de faire vérifier les données par le prestataire de messagerie.

4.2.4 Portugal

4.2.4.1 Le cadre juridique et son étendue

196 La loi portugaise sur la cybercriminalité (loi nº 109/2009 du 15 septembre 2009) définit les « cybercrimes » et réglemente l'obtention de preuves électroniques. Sa structure et son contenu correspondent globalement à ceux de la Convention de Budapest.

197 En vertu de l'article 11 de la loi sur la cybercriminalité, la plupart des règles de procédure pénale habituelles s'appliquent aussi à des infractions « commises au moyen d'un système informatique » et aux enquêtes nécessitant « de recueillir des preuves sous forme électronique ». Cet article s'inspire de l'article 14.2 de la Convention de Budapest. L'interception des communications et les enquêtes par infiltration sont réglementées par la législation générale, mais peuvent aussi être utilisées pour les enquêtes sur les infractions couvertes par la loi sur la cybercriminalité.

4.2.4.2 Perquisitions transfrontalières

198 La loi portugaise sur la cybercriminalité autorise l'accès transfrontalier aux données dans le contexte de la perquisition de données informatiques. Les règles en matière de perquisition, énoncées principalement à l'article 15 de la loi, s'inspirent à la fois du Code portugais de procédure pénale et de la Convention de Budapest. En vertu de l'article 15.1, un juge peut autoriser la perquisition d'un système informatique lorsqu'elle est nécessaire, dans le cadre d'une procédure, pour recueillir des preuves, établir la vérité et recueillir des données sûres et spécifiques stockées dans un système précis.

199 En outre, en vertu de l'article 15.5, si au cours d'une perquisition il y a des raisons de croire que les informations recherchées sont stockées sur un autre système informatique ou dans une partie différente du système initial, tout en étant légalement accessibles depuis le système initial, la perquisition peut être étendue, avec l'autorisation de l'autorité compétente. Le texte de l'article ne fixe aucune limite « géographique » ou juridictionnelle à cette mesure procédurale. L'extension s'applique aux systèmes situés à l'intérieur comme en dehors des frontières portugaises.

200 En pratique, l'extension prévue à l'article 15 peut s'appliquer à la perquisition de systèmes étendus (comme le système d'une grande entreprise) lorsqu'il s'avère que les données recherchées sont physiquement stockées en un lieu éloigné. Elle s'applique aussi à l'accès à des messageries électroniques. Dans les deux cas, il est possible d'accéder à des systèmes physiquement situés à l'intérieur ou en dehors du territoire portugais. Bien sûr, cette possibilité juridique dépend de la question de savoir si l'accès au système initial est légalement autorisé ou non.

201 Cette disposition transpose clairement en droit portugais l'article 19.2 de la Convention de Budapest, qui demande à toutes les Parties à la Convention d'adopter les mesures nécessaires

pour veiller à ce que, lors de la perquisition d'un système informatique, les autorités puissent étendre la perquisition à un autre système si elles ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique. Cependant, l'article 19.2 ne prévoit que l'extension des recherches aux données stockées sur le territoire des autorités concernées.

202 Sur ce point, le cadre juridique portugais va au-delà des dispositions de la Convention de Budapest : l'article 15.5 de la loi sur la cybercriminalité n'établit pas de différence entre l'extension d'une perquisition à des systèmes « nationaux » et à des systèmes physiquement situés en dehors du territoire portugais. Les forces de l'ordre portugaises peuvent donc légitimement accéder à des données physiquement situées dans un système éloigné, à l'étranger, si elles en ont dûment reçu l'ordre (habituellement de la part du procureur, mais aussi du juge dans certaines affaires, conformément aux paragraphes 1 et 6 de l'article 15).

203 Concernant la validité des preuves ainsi obtenues, en l'absence de réglementation spécifique, la règle générale énoncée à l'article 125 du Code portugais de procédure pénale s'applique. L'article 125 affirme que toutes les preuves non interdites par la loi sont recevables.

204 Comme déjà évoqué, il est permis, au cours de perquisitions nationales, d'accéder à des données physiquement situées sur tout autre territoire au moyen d'une extension de perquisition. Cette possibilité procédurale reste légitime lorsqu'un membre des autorités répressives d'un autre Etat accède à des données physiquement situées sur le territoire portugais. En pareil cas, l'article 25 de la loi sur la cybercriminalité affirme :

> Les autorités étrangères compétentes peuvent, sans autorisation préalable des autorités portugaises, accéder à des données stockées dans un système informatique physiquement situé au Portugal. Cette démarche est autorisée lorsque les données sont publiques (article 25, 1er alinéa) et lorsque les autorités de l'Etat concerné ont obtenu le consentement légal et volontaire de la personne légalement autorisée à divulguer les données (article 25b).

205 Cette disposition transpose en droit portugais l'article 32 de la Convention de Budapest.

206 La définition d'un « système informatique » en droit portugais est très large. En vertu de l'article 2a de la loi sur la cybercriminalité, on entend par « système informatique » tout équipement ou ensemble d'équipements connectés ou reliés entre eux où au moins l'un des éléments comporte des logiciels ou traite automatiquement des données. Cette définition large amplifie les possibilités d'extension des perquisitions.

4.2.4.3 **Saisie transfrontalière de données**

207 La saisie de données informatiques est elle aussi réglementée. En général, conformément au Code portugais de procédure pénale, la saisie est une mesure procédurale appliquée pour conserver les preuves d'une infraction pénale ou pour geler ou confisquer les produits d'un crime. La loi sur la cybercriminalité (article 16) décrit spécifiquement la saisie de données informatiques. Elle est liée à l'accès transfrontalier à des données informatiques.

208 En fait, une perquisition est par nature une mesure procédurale dont l'objectif est de saisir des preuves ou des produits d'un crime. Par conséquent, la perquisition d'un système informatique vise également la saisie de données.

209 Par ailleurs, la saisie peut également se produire en l'absence de perquisition, si les autorités ont des raisons de penser qu'il est nécessaire de conserver les preuves ou les produits d'un crime. Ce

peut être le cas dans l'environnement numérique, à condition que l'accès au système ait été volontairement consenti. Pour qu'il y ait consentement volontaire, il faut que le propriétaire du système ou la personne légalement autorisée à fournir l'accès au système donne son accord aux autorités répressives. En vertu du droit portugais, cela s'applique aux systèmes situés aussi bien à l'intérieur qu'en dehors des frontières portugaises, si l'accès à ces systèmes est légalement autorisé. Une fois l'accès obtenu, la saisie peut être exécutée.

210 A travers ce mécanisme, la législation portugaise adopte, en matière d'enquêtes pénales nationales, les dispositions de l'article 32b de la Convention de Budapest.

211 Cette mesure procédurale requiert un ordre du procureur ou l'approbation d'un juge dans des cas spécifiques, par exemple la saisie de messages électroniques (article 17 de la loi sur la cybercriminalité). L'intervention d'un juge est toujours requise en cas de saisie de données ou de documents informatiques susceptibles de contenir des renseignements personnels ou intimes et de compromettre la vie privée de leur propriétaire ou de tiers.

212 Conformément à l'article 16.7 de la loi portugaise sur la cybercriminalité, la saisie de données peut prendre plusieurs formes différentes. Elle peut se faire physiquement, par la saisie du matériel où les données sont stockées, en copiant les données, en conservant les données telles quelles (sans les copier ni les supprimer) et enfin, en supprimant temporairement les données ou en bloquant l'accès aux données.

213 En droit portugais, les « données informatiques » ont une définition large. On entend par « donnée informatique » toute représentation de faits, informations ou concepts sous un format pouvant être traité au moyen d'un système informatique, y compris les programmes qui permettent à un système informatique d'accomplir une fonction.

4.2.5 Roumanie

4.2.5.1 **Cadre juridique**

214 Le droit roumain établit une distinction entre la perquisition d'ordinateurs et l'accès à un système informatique. Tandis que la perquisition d'ordinateurs[85] est menée si possible en présence du suspect et de son avocat, l'accès à un système informatique est considéré comme un moyen spécial d'enquête, comparable à l'interception d'une communication, et peut être exécuté en secret.

215 L'article 57 de la loi n° 161/2003 assimile l'accès à un système informatique à l'interception ou à l'enregistrement de communications. Cette mesure requiert un mandat judiciaire. Les conditions sont les suivantes :

- la mesure est nécessaire pour découvrir la vérité ;
- il n'est pas possible d'établir les faits, d'identifier les auteurs de l'infraction ou de les localiser au moyen d'autres preuves ;
- la mesure porte sur un crime grave[86].

[85] Certaines des conditions énoncées pour les perquisitions de domiciles s'appliquent aussi aux perquisitions d'ordinateurs (articles 100 et suiv. du Code roumain de procédure pénale).

[86] La notion de « crime grave » est définie par la loi n° 39/2003, article 2, alinéa b, sous la forme d'une liste d'infractions. Conformément au point 20 de cette liste, est considérée comme un crime grave toute autre infraction pour laquelle la loi prévoit une peine minimale de prison d'au moins cinq ans. Le point 18 nomme

216 Dans les cas urgents, par exemple si l'attente d'un mandat judiciaire retarderait fortement les poursuites pénales, le procureur peut ordonner l'interception de toute communication ou de l'accès à un système informatique pour une période de 48 heures. La mesure provisoire ordonnée par le procureur doit être présentée à un tribunal pour validation dans les 48 heures suivant son expiration. Le juge peut partager ou non l'analyse du procureur quant à l'urgence de la situation. Si le juge y consent, une nouvelle autorisation est délivrée pour une durée de 28 jours. Si non, l'autorisation est annulée et les documents obtenus doivent être détruits.

4.2.5.2 **Application pratique**

217 Le droit procédural s'applique à l'égard d'un territoire et d'une personne et en lien avec une infraction donnée. Pour définir la juridiction compétente, le procureur tient compte de la compétence matérielle (nature de l'infraction, nationalité de son auteur, agissements commis au niveau national ou à l'étranger etc.) ainsi que de la compétence territoriale, en fonction des divisions administratives roumaines ou du lieu de résidence de l'auteur si l'infraction a été commise à l'étranger.

218 S'agissant de l'interception et de l'enregistrement d'une conversation téléphonique ou d'autres types de communications, si le procureur formule une telle demande, son mandat peut prévoir :

- l'interception et l'enregistrement d'un terminal de communication utilisant un numéro d'identification roumain opérant en Roumanie ou en itinérance (voix/données) ;
- l'interception et l'enregistrement d'un terminal de communication utilisant un numéro d'identification étranger et opérant en Roumanie ou en itinérance (voix/données) ;
- l'accès à un système informatique, si la connexion à l'ordinateur peut être établie depuis la Roumanie en utilisant des réseaux nationaux ou interconnectés (le principe de l'itinérance s'applique : le service principal est fourni depuis la Roumanie ou depuis l'étranger mais est relié au réseau national, si bien que le service est disponible depuis la Roumanie).

219 L'ordre est exécuté en Roumanie par le procureur ou par la police, avec l'aide technique d'une unité spéciale ou du prestataire de services situé en Roumanie.

220 Lorsque la mesure ne peut être techniquement exécutée en Roumanie, l'ordre fait l'objet d'une lettre rogatoire envoyée à l'autorité judiciaire compétente, afin d'en assurer la bonne exécution.

4.2.6 Serbie

4.2.6.1 **Cadre juridique**

221 En Serbie, une « loi sur l'organisation et les compétences des autorités gouvernementales dans la lutte contre la cybercriminalité » a été adoptée par l'Assemblée nationale en juin 2005. Elle a créé des instances spécialisées au sein du ministère de l'Intérieur, du parquet et du système judiciaire. La première instance créée a été la Chambre spéciale du parquet pour la criminalité de haute technologie, début 2006, suivie du Département spécial pour la criminalité de haute technologie au sein du Service de lutte contre le crime organisé du ministère de l'Intérieur et par des unités

---

parmi les crimes graves des infractions commises via des systèmes et réseaux de communication, y compris numériques.

spéciales de poursuites et d'enquête au sein du Tribunal de deuxième instance de Belgrade. Conformément à l'article 3 de la loi, ces instances sont compétentes pour lutter contre la criminalité dans tout le pays.

222 Outre cette loi, les dispositions d'autres lois s'appliquent aussi à la cybercriminalité : Code pénal, loi sur les poursuites pénales, version actuelle du Code de procédure pénale, loi sur les communications électroniques, loi sur l'entraide judiciaire en matière pénale etc.

223 S'agissant de l'accès à des données informatiques au cours d'enquêtes préliminaires ou de poursuites pénales, les instances susmentionnées doivent observer les définitions et la procédure énoncées par le Code pénal et par le Code de procédure pénale, où la notion de biens meubles englobe les données et programmes informatiques. Le Code de procédure pénale serbe est très clair concernant la perquisition et la saisie de locaux et d'objets liés à l'exécution d'une infraction pénale : il ne peut y avoir perquisition de locaux et autres lieux liés à des accusés ou à d'autres personnes que s'il est probable qu'elle aboutira à l'arrestation de l'accusé ou à la détection de preuves d'une infraction pénale ou d'objets importants pour la procédure pénale.

224 La perquisition est ordonnée par un tribunal au moyen d'un ordre de perquisition écrit et motivé. Les objets à saisir en vertu du Code pénal ou susceptibles de constituer des preuves dans une procédure pénale sont saisis et placés en lieu sûr, que ce soit au sein du tribunal ou ailleurs.

225 Dans sa version actuelle, le Code de procédure pénale serbe (« CPP ») prévoit des techniques d'enquête spéciales pouvant être utilisées pour accéder à un ordinateur et aux données afférentes, telles que la surveillance et l'enregistrement de communications téléphoniques ou d'autres modes de communication et les recherches informatiques automatisées de données personnelles et autres. La nouvelle version du CPP (déjà appliquée par les Bureaux de poursuite du crime organisé et des crimes de guerre) met encore davantage de techniques et mesures d'enquête à la disposition des autorités répressives et du parquet pour qu'ils puissent accéder à des données informatiques relatives à des actes criminels.

226 Le CPP serbe reconnaît les données informatiques comme telles et ne différencie pas les données présentes dans des ordinateurs et systèmes informatiques serbes ou étrangers, du moment que ces données permettent de détecter des preuves d'une infraction pénale ou représentent sous forme électronique des objets qui seront importants pour la procédure pénale, que les autres conditions de perquisition et de saisie énoncées dans le CPP sont remplies et que l'auteur de l'infraction peut être poursuivi en vertu des dispositions du Code pénal et du Code de procédure pénale serbes.

227 Les dispositions de la loi serbe sur les communications électroniques réglementent en outre la confidentialité des communications électroniques ainsi que l'interception et la conservation légales des données. Cette loi énonce de très importantes obligations à respecter par les prestataires de services Internet, facilitant un accès fiable aux données au cours de procédures pénales.

4.2.6.2 **Application pratique**

228 L'accès transfrontalier, possible dans différentes situations, est exécuté par le Département spécial pour la criminalité de haute technologie. Il peut s'agir d'un accès transfrontalier pendant une perquisition de locaux, au moyen de mots de passe obtenus légalement ou avec le consentement de la personne autorisée ou de l'obtention d'informations auprès d'un prestataire de services, à l'exclusion de l'accès transfrontalier au moyen de logiciels ou moyens techniques spéciaux.

229 L'utilisation d'un mot de passe obtenu légalement et le consentement de la personne autorisée sont les deux cas d'accès transfrontalier les plus fréquents en Serbie. Cette pratique des autorités répressives n'a pas été contestée à ce jour.

230 L'un des grands principes sous-jacents est que, bien que le système ou serveur interrogé puisse se trouver à l'étranger, les données consultées elles-mêmes ont été transférées sur l'ordinateur situé dans les locaux de l'auteur de l'infraction en Serbie. Ces données sont donc, de façon temporaire ou définitive, stockées au sein de la juridiction territoriale des autorités serbes.

4.2.7 Etats-Unis

231 Les enquêteurs et procureurs étasuniens disposent de pouvoirs juridiques et procéduraux étroitement définis pour obtenir des données informatiques stockées en dehors des Etats-Unis. Dans la pratique, ces lois et procédures limitent significativement l'accès transfrontalier de la part des autorités répressives étasuniennes.

232 Le plus souvent, pour obtenir des données informatiques stockées à l'étranger, les autorités répressives étasuniennes coopèrent avec le gouvernement de l'Etat concerné. Les principaux mécanismes à cet effet sont l'entraide judiciaire ou les lettres rogatoires, ou encore des actions menées en commun par les autorités répressives des deux Etats. Ce mode coopératif d'accès transfrontalier permet aux enquêteurs et procureurs étasuniens d'obtenir presque toutes les données voulues, dont notamment des données de contenu transmises par d'autres Etats.

233 Les autorités répressives des Etats-Unis collectent également des données stockées à l'étranger via des méthodes énoncées à l'article 32 de la Convention sur la cybercriminalité. L'une des pratiques courantes aux Etats-Unis consiste à accéder à des données publiquement disponibles sur Internet, indépendamment de la situation géographique du site Internet, de l'hébergeur du site ou de la personne[87] qui possède ou contrôle les données. Cette pratique est réglementée par les lois générales applicables aux enquêtes pénales, dont la Constitution (qui protège les droits individuels), le Code pénal et le Code de procédure pénale fédéraux[88] et les décisions de justice interprétant ces dispositions. En outre, le ministère de la Justice et d'autres autorités chargées de l'application de la loi ont promulgué des orientations spécifiques concernant les enquêtes en ligne.

234 Les enquêteurs étasuniens peuvent aussi accéder à des données stockées sur un ordinateur à l'étranger après avoir obtenu le consentement légal et volontaire de la personne légalement autorisée à divulguer ces données via cet ordinateur. Le plus souvent, ce type d'accès transfrontalier se produit lorsqu'un enquêteur obtient le consentement d'un individu ou d'une entreprise se trouvant aux Etats-Unis mais contrôlant des données pertinentes pour l'enquête dans un autre Etat. Généralement, l'enquêteur et la personne qui détient ou contrôle les données coopèrent pour accéder aux données et les récupérer. Comme pour l'accès aux données publiques, cette pratique est régie par les lois et procédures étasuniennes, la nature et l'étendue du consentement volontaire laissant largement la place à l'interprétation judiciaire. L'article 32 de la Convention sur la cybercriminalité fournit également une base à cette pratique. Cependant, les lois étasuniennes limitent la capacité des tiers à divulguer volontairement des informations au gouvernement[89]. Lorsque le droit des Etats-Unis interdit la divulgation volontaire, la solution de

[87] Dans ce chapitre, « personnes » renvoie aussi bien aux personnes physiques que morales.

[88] Code des Etats-Unis, Titre 18, *Infractions et procédures pénales.*

[89] Voir par exemple la loi sur les communications stockées (Code des Etats-Unis, Titre 18, articles 2701-2712), la loi sur le droit à la confidentialité financière (Code des Etats-Unis, Titre 12, articles 3401-3422) et

l'accès transfrontalier par consentement se ferme puisque la personne (prestataire de services par exemple) n'est pas habilitée à divulguer les données, où qu'elles se trouvent.

235 L'article 18 de la Convention sur la cybercriminalité et le droit étasunien autorisent le gouvernement à demander, en promulguant un ordre en ce sens, la divulgation de données stockées dans un autre Etat si elles ont un lien avec l'enquête et sont contrôlées par une personne ou par une entité physiquement située aux Etats-Unis. Pour obtenir des données stockées à l'étranger, le gouvernement étasunien préfère nettement, lorsque c'est possible, coopérer avec les autres Etats. Le ministère de la Justice des Etats-Unis demande donc aux procureurs de n'ordonner la production de telles données qu'après avoir obtenu l'approbation d'un haut responsable du ministère. La question de savoir quand une personne présente sur un territoire peut être enjointe de produire des informations qu'elle possède ou contrôle, mais qui se trouvent sur un autre territoire précède de loin non seulement la Convention, mais aussi l'apparition même des ordinateurs. Les Etats-Unis traitent donc des demandes de ce type depuis une époque bien antérieure à l'apparition d'Internet.

236 Les autorités répressives étasuniennes peuvent procéder, bien que beaucoup moins fréquemment, à d'autres types d'accès transfrontalier, notamment lorsque l'emplacement des données stockées n'est pas connu ou lorsque les enquêteurs n'avaient pas prévu que les recherches s'étendraient au-delà du territoire des Etats-Unis. L'article 39 de la Convention sur la cybercriminalité (ainsi que les paragraphes 293 et 314 du Rapport explicatif) prévoient que les cas de recherches transfrontalières dépassant ceux couverts par les articles 18 et 32 ne sont ni spécifiquement autorisés, ni exclus.

4.3 Accès via des prestataires et d'autres entités privées

4.3.1 Pratiques

237 Dans les scénarios décrits aux chapitres précédents, les autorités répressives accédaient à des données informatiques avant tout de façon directement transfrontalière. Le scénario le plus courant, cependant, semble être que les autorités répressives obtiennent l'accès à des données stockées à l'étranger en coopérant avec des prestataires de services ou avec d'autres entités du secteur privé.

238 Comme indiqué précédemment dans ce rapport, l'article 32b n'exclut pas que la personne autorisant de façon « légale et volontaire » la divulgation des données soit une entité privée ayant le contrôle de ces données.

239 En Europe par exemple, plusieurs prestataires de services étasuniens ayant des succursales en Europe ont mis en place des accords volontaires (« programmes de conformité pénale ») entre leurs bureaux européens et les autorités répressives de certains gouvernements, en vertu desquels ces bureaux peuvent divulguer des données sous certaines conditions et sans que le gouvernement concerné n'adresse de demande d'entraide judiciaire au ministère de la Justice des Etats-Unis. Les conditions fixées pour ces demandes de « conformité volontaire » sont généralement les suivantes :

---

les règles de confidentialité de la loi de 1996 sur la transparence et la portabilité de l'assurance maladie (loi publique n° 104-191 et Code des règlements fédéraux, Titre 45, parties 160 et 164).

- La demande doit être légale et émaner d'une autorité ayant compétence sur l'affaire concernée ; un cadre juridique clair doit être en place concernant les enquêtes sur la cybercriminalité et la collecte de preuves électroniques.
- Les données demandées doivent avoir un lien avec le territoire des autorités répressives à l'origine de la demande (via les adresses IP d'une communication, le pays du nom de domaine d'un compte de messagerie etc.).
- Les agissements objets de l'enquête doivent aussi constituer une infraction aux Etats-Unis (principe de double incrimination, destiné à exclure les infractions politiques ou les enquêtes portant sur la liberté d'expression).
- Dans la plupart des cas, seules les données détenues et contrôlées par les prestataires – comme les données de trafic ou d'inscription – sont divulguées, mais non le contenu généré par les usagers (pour ces contenus, une demande officielle d'entraide judiciaire est nécessaire[90]).
- Le système de justice pénale de l'Etat est supposé respecter les normes internationales en matière de droits de l'homme et de prééminence du droit, y compris la protection de la vie privée.

240 Les entités privées peuvent aussi être officiellement enjointes d'obéir à des ordres de perquisition, de saisie et de production prononcés en vertu de la législation des Etats dans lesquels elles opèrent[91].

241 L'obligation de donner suite à de telles demandes judiciaires peut entrer dans le champ des pouvoirs nationaux prévus aux articles 18 et 19 de la Convention de Budapest, mais ne constitue pas un « consentement volontaire » au sens de l'article 32b.

242 Il paraît clair que les entités privées actives dans différents pays sont soumises à des législations multiples et que le respect de la législation d'un pays peut les amener à enfreindre celle d'autres pays. Elles doivent résoudre, en particulier, des conflits avec les principes des droits de l'homme et de la prééminence du droit.

4.3.2 Préoccupations

243 Plusieurs parties prenantes ont exprimé des préoccupations, telles que celles qui suivent[92].

4.3.2.1 **Global Network Initiative**

244 L' « Initiative Réseau mondial » résume le problème comme suit :

> Dans le monde entier, des Amériques à l'Europe en passant par le Moyen-Orient, l'Afrique et l'Asie, les entreprises du secteur des TIC (technologies de l'information et de la communication)

[90] Il semble que certains prestataires puissent aussi divulguer des données de contenu si un mandat judiciaire officiel est émis et si l'usager, en s'inscrivant, a accepté les conditions correspondant à l'Etat des autorités répressives demandeuses.

[91] Ces demandes officielles ne sont pas couvertes par l'article 32 de la Convention de Budapest mais par les dispositions sur les pouvoirs répressifs nationaux, comme la perquisition et la saisie (article 19) ou les injonctions de produire (article 18), si la demande est liée à une enquête pénale. L'une des principales préoccupations semble être la possibilité que des données soient réclamées en vertu de législations sur le renseignement intérieur ou la sûreté nationale qui offrent peu de garanties de protection des droits de l'homme et de la prééminence du droit.

[92] Ces préoccupations sont relayées ici pour alimenter le débat. Elles ne reflètent pas nécessairement le point de vue du Groupe sur l'accès transfrontalier.

> sont de plus en plus pressées par les gouvernements d'obéir aux lois et aux politiques nationales, au prix de potentielles violations de droits fondamentaux tels que la liberté d'expression ou le respect de la vie privée[93].

245 GNI a adopté une série de principes à suivre par les entreprises pour protéger la vie privée et la liberté d'expression.

246 Récemment, il a été proposé que les demandes de données stockées sur des serveurs à l'étranger passent toujours par une procédure d'entraide judiciaire[94].

4.3.2.2 **Déclaration de la Chambre de commerce internationale (ICC)**

247 La Chambre de commerce internationale (ICC) a publié en 2012 une déclaration dans laquelle elle relève :

> De plus en plus, les entreprises qui gèrent des données dans de multiples pays sont soumises aux pressions de gouvernements pour qu'elles répondent à des demandes d'accès à des données personnelles, formulées par les autorités répressives ou par d'autres instances officielles, qui entrent en conflit avec les lois sur la protection des données et de la vie privée en vigueur dans d'autres pays où elles sont actives[95].

248 Voici un exemple donné par l'ICC :

> Exemple 1 : l'entreprise X est active dans de nombreux pays dont le pays A, dont la législation ne protège pas correctement les données personnelles. Elle transfère des données personnelles liées à des transactions dans le monde entier vers sa base de données centrale, située à son siège dans le pays B. L'entreprise X a pris les mesures nécessaires pour que ses activités de traitement des données respectent les obligations juridiques des pays dans lesquels elle est active. Entre autres, elle s'est engagée à limiter l'usage des données aux fins exposées au moment où elles ont été recueillies, et à ne les transmettre à des tiers que sur une base juridique et si des mesures sont prises pour que les données soient correctement protégées dans le pays vers lequel elles sont transférées. En outre, la politique de confidentialité de l'entreprise X à l'égard de sa clientèle affirme que les données personnelles ne seront utilisées qu'à des fins précises et très limitées et prévoit une protection adéquate en cas de communication de ces données.
> Les autorités répressives du pays A contactent l'entreprise X, affirmant soupçonner des activités illégales de la part de certaines personnes avec lesquelles l'entreprise est en affaires. Ces personnes sont ressortissantes de nombreux pays différents, y compris le pays A. Les mêmes autorités demandent ensuite à l'entreprise X de leur livrer tous les fichiers qu'elle possède concernant des transactions avec ces personnes au cours des trois dernières années, y compris les fichiers stockés dans sa base de données dans le pays B. La demande ne se fonde pas sur un mandat judiciaire et ne mentionne que les noms des personnes concernées et le laps de temps au

---

[93] http://www.globalnetworkinitiative.org/

[94] Brown, Ian/Korff, Douwe (2012) : « Digital Freedoms in International Law – Steps to Protect Human Rights Online » (rapport élaboré pour Global Network Initiative, GNI) https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

[95] « ICC Policy Statement: Cross-border law enforcement access to company data – current issues under data protection and privacy law » (février 2012), disponible sur http://www.iccwbo.org/Advocacy-Codes-and-Rules/Document-centre/2012/ICC-policy-statement-on-cross-border-law-enforcement-access-to-company-data---current-issues-under-data-protection-and-privacy-law/

cours duquel les transactions ont eu lieu. Les autorités préviennent que s'il n'est pas donné suite à leur demande, elles ouvriront une procédure pénale contre la direction de la filiale de l'entreprise X dans le pays A.

249 D'après l'ICC, de telles pressions peuvent avoir plusieurs conséquences : conflits avec les législations en matière de protection de la vie privée et des données personnelles, violation des engagements de l'entreprise envers ses employés et ses clients, risques de tensions politiques et impact sur les décisions commerciales.

250 Par conséquent, l'ICC « appelle les autorités répressives et les gouvernements à prendre les initiatives suivantes » :

- Tenir compte de la possibilité que les demandes des autorités répressives entrent en conflit avec la législation d'autres pays en matière de protection des données personnelles ou de la vie privée.
- N'adresser les demandes d'accès aux données que par écrit et conformément au droit écrit et/ou à la réglementation locale, plutôt que de façon informelle. Indiquer clairement pour toute demande sur quelle base juridique précise elle se fonde et le nom de l'autorité officielle à l'origine de la demande.
- Adresser les demandes de données stockées dans un autre pays par le biais des accords et procédures d'entraide judiciaire, au sein des cadres existants, en veillant à y associer suffisamment les autorités des pays où les données sont stockées. Les textes existants en matière d'entraide judiciaire devraient aussi être améliorés, afin (1) de couvrir les nouveaux services de communications par adresse IP ; (2) de permettre la livraison des données demandées dans des délais satisfaisants pour les autorités répressives ; (3) d'améliorer la sécurité juridique concernant le respect des différentes législations nationales ; (4) de donner suffisamment d'informations aux entreprises pour qu'elles puissent participer efficacement au processus d'entraide judiciaire, et (5) de créer un point de contact unique au sein des autorités répressives de chaque pays.
- Donner aux entreprises la possibilité de vérifier la légitimité de la demande et d'informer les autorités (y compris leurs propres autorités nationales) de leurs obligations en vertu de la législation sur la protection des données personnelles et de la vie privée, le cas échéant.
- Être aussi précis et concis que possible quant à l'étendue de la demande (par exemple, quelles données les autorités recherchent et sur quel laps de temps) et réduire au maximum la quantité de données demandées.
- S'abstenir de développer des mécanismes qui obligent une entreprise à s'engager, soi-disant « volontairement », à livrer des informations sous la menace de sanctions importantes (pénales, financières ou fiscales) ou de l'arrêt des relations commerciales avec cette entreprise.
- Permettre aux entreprises de limiter leur responsabilité potentielle, par exemple en masquant ou en rendant anonymes les données personnelles de tierces parties qui ne sont pas concernées par l'enquête.

La mise en œuvre de ces recommandations permettrait aux entreprises de répondre plus efficacement aux demandes légitimes des autorités répressives et des autres autorités publiques et de mieux faire face à des obligations juridiques contradictoires. Elle favoriserait le respect des lois en matière de protection des données et de la vie privée et stimulerait le commerce international en répondant aux besoins croissants de sécurité juridique des entreprises qui souhaitent planifier des investissements.

4.3.2.3 **Livre blanc sur l'accès des pouvoirs publics aux données en ligne[96]**

251 D'après ce livre blanc, élaboré par le cabinet d'avocats Hogan Lovells[97], beaucoup de gouvernements peuvent demander aux prestataires de services en ligne de leur pays de fournir des informations stockées sur des serveurs à l'étranger :

- Australie : les demandes de données adressées à des entreprises et organisations australiennes s'étendent aux données situées sur des serveurs en dehors de l'Australie, à condition que l'infraction pénale présumée ou le problème de sécurité objet de la demande se soit produit entièrement ou partiellement en Australie ou concerne des ressortissants ou résidents australiens. Le gouvernement australien peut donc demander à un prestataire de services en ligne de lui fournir des données de serveurs étrangers aussi bien qu'australiens.

- Canada : les demandes de données émanant du Canada ne se limitent pas aux données situées dans le pays. En général, les entreprises relevant du ressort du Canada sont tenues de remettre toutes les données pertinentes qu'elles « détiennent ou contrôlent », soit parce qu'elles peuvent accéder aux données elles-mêmes, soit parce qu'elles peuvent demander à un tiers (tel qu'une filiale) d'y accéder ou de les produire. Le gouvernement canadien peut donc demander à un prestataire de services en ligne de lui fournir des données de serveurs étrangers aussi bien que canadiens.

- Danemark : si un prestataire danois de services en ligne stocke des données relatives à sa clientèle sur des serveurs situés à l'étranger, le gouvernement peut accéder à ces données sur ordre de perquisition, à condition qu'elles puissent être atteintes et consultées à partir du site du prestataire au Danemark. Autrement, la marge d'action du gouvernement danois concernant l'accès à des données sur des serveurs étrangers dépend de son niveau de coopération judiciaire avec les pays concernés.

- France : le droit français autorise expressément les pouvoirs publics à obtenir toute information pertinente pour une enquête à partir d'un système informatique à condition que les données soient accessibles depuis ce système. Le gouvernement français peut donc demander à un prestataire de services en ligne de lui fournir des données de serveurs étrangers aussi bien que français.

- Allemagne et Japon : il n'est pas possible d'accéder à des données à l'étranger.

- Irlande : du moment que l'Irlande peut établir sa compétence sur une entité, les autorités irlandaises peuvent demander à cette entité de fournir des données relatives à sa clientèle à partir d'un serveur situé dans un autre pays mais placé sous son contrôle. Le gouvernement irlandais peut donc demander à un prestataire de services en ligne de lui fournir des données de serveurs étrangers aussi bien qu'irlandais.

---

[96] Maxwell, Winston/Wolf, Christopher (2012) : « A Global Reality: Governmental Access to Data in the Cloud » (Livre blanc d'Hogan Lovells, 23 mai 2012) http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf

[97] Winston Maxwell, co-auteur du livre blanc, a participé à la Conférence Octopus (atelier sur l'accès transfrontalier aux données) en juin 2012. Les participants à cet atelier ont souhaité souligner que ce document ne reflétait pas nécessairement le point de vue des autorités concernées dans les Etats étudiés.

- Royaume-Uni : lorsque les autorités gouvernementales britanniques disposent d'un mandat de perquisition de données électroniques, elles peuvent demander la recherche de toutes les informations présentes sur un ordinateur et accessibles depuis les locaux perquisitionnés. En d'autres termes, du moment que les serveurs étrangers sont accessibles depuis des locaux se trouvant au Royaume-Uni, la police peut demander au prestataire de services en ligne de lui remettre également des données stockées sur des serveurs étrangers.

- Etats-Unis : comme d'autres pays, les Etats-Unis se jugent habilités à utiliser leurs propres mécanismes juridiques pour obtenir des données de serveurs situés n'importe où dans le monde, du moment que le prestataire de services en ligne relève de leur ressort — c'est-à-dire si l'entité se trouve aux Etats-Unis, dispose de succursales ou de bureaux aux Etats-Unis ou mène des activités régulières et continues aux Etats-Unis.

252 Lors du débat sur ce livre blanc au cours de la Conférence Octopus, en juin 2012[98], il a été jugé que certaines de ses conclusions pouvaient être controversées et surestimaient les pouvoirs des autorités répressives. Dans la plupart des Etats, de nombreuses conditions doivent être remplies pour que les autorités puissent ordonner à une entité privée de leur communiquer des données. Il peut être obligatoire, par exemple, que l'adresse IP soit reliée au territoire des autorités répressives, que le suspect se trouve sur ce territoire ou que la demande fasse l'objet de contrôles juridictionnels et autres[99]. Il serait faux de considérer qu'il existe un accès sans restrictions.

[98] www.coe.int/octopus2012

[99] S'agissant des Etats-Unis, le livre blanc extrapole trop le point de vue étasunien quant à la compétence des autorités du pays. Tous les procureurs fédéraux étasuniens doivent demander par écrit l'autorisation d'affirmer leur compétence lorsque le seul lien avec les Etats-Unis est la présence d'un bureau ou d'une succursale. Voir : US Attorneys' Manual, http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm00279.htm. De telles demandes d'autorisation sont peu fréquentes.

5 Comment aller au-delà de l'article 32b ?

253 A l'époque où le principe de l'accès transfrontalier avec consentement était négocié au sein du G8 et du Conseil de l'Europe, d'autres solutions étaient déjà envisagées pour couvrir les situations d'accès transfrontalier sans consentement ou les cas dans lesquels l'emplacement des données ou des systèmes n'était pas connu. Ce dernier point a récemment gagné en importance avec l'essor du *cloud computing* (informatique décentralisée) et la « disparition du lieu » qu'elle entraîne.

254 Nous résumons ici certaines propositions, afin d'alimenter la réflexion et de fournir des éléments pour trouver d'autres solutions que l'article 32b. Elles n'excluent bien sûr pas d'autres propositions.

Proposition 1 : accès transfrontalier avec consentement non limité aux données stockées dans une autre Partie

255 Des dispositions supplémentaires pourraient s'avérer nécessaires pour couvrir les situations dans lesquelles le consentement est donné dans des conditions proches de celles de l'article 32b, mais lorsqu'on ignore où les données se trouvent ou quelle trajectoire elles suivent exactement[100].

256 Il a en outre été proposé d'élargir le champ de l'article pour autoriser l'accès à des données situées dans des Etats non Parties à la Convention.

Proposition 2 : accès transfrontalier sans consentement mais par des moyens obtenus légalement

257 Une nouvelle disposition pourrait être ajoutée à la Convention de Budapest (par le biais d'un Protocole additionnel)

> autorisant une Partie, sans l'autorisation d'une autre Partie, à consulter ou à recevoir à partir d'un système informatique situé sur son territoire, au cours d'une enquête ou d'une procédure pénale, des données informatiques stockées dans une autre Partie, si elle en a obtenu les moyens grâce à des activités d'enquête légales. La Partie enquêtrice en avertit l'autre Partie avant, pendant ou après l'acquisition des données.

Proposition 3 : accès transfrontalier sans consentement de bonne foi ou dans des situations urgentes ou exceptionnelles

258 Une nouvelle disposition pourrait être ajoutée à la Convention de Budapest pour autoriser l'accès transfrontalier dans des situations spécifiques, c'est-à-dire pour empêcher un danger imminent, une atteinte à l'intégrité physique, l'évasion d'un suspect etc. Ces situations pourraient aussi englober le risque de destruction de preuves pertinentes. Là encore, cela supposerait de définir des garanties et des critères spécifiques et de prévoir la notification de l'autre Partie.

259 Une nouvelle disposition pourrait également couvrir les actes « de bonne foi », c'est-à-dire les situations où, au cours d'une perquisition, les autorités répressives n'ont pas la certitude que le système perquisitionné se trouve à l'étranger, soit ignorent sur quel territoire il se trouve soit ont obtenu des preuves situées à l'étranger par erreur ou par accident.

[100] Comme relevé plus haut dans ce rapport, l'article 32b sous sa forme actuelle ne s'applique qu'aux situations où les données sont stockées dans une autre Partie.

Proposition 4 : extension des perquisitions sans restriction au territoire de l'Etat enquêteur

260 Comme expliqué plus haut dans ce rapport, l'article 19.2 de la Convention de Budapest demande aux Parties d'autoriser l'élargissement des perquisitions aux systèmes informatiques connectés au système initial, mais en se limitant à leur territoire :

> 2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire[101], et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

261 Il serait imaginable d'abandonner cette restriction[102]. Cependant, des critères et des garanties spécifiques devraient être définis.

Proposition 5 : le pouvoir d'utilisation[103], critère de légalité des recherches

262 On a parlé de « disparition du lieu » pour qualifier les situations dans lesquelles il est très difficile, voire impossible d'attribuer un emplacement spécifique à des données. Les données sont « quelque part en ligne » ; elles peuvent passer d'un serveur ou d'un lieu à l'autre, être réparties entre différents lieux ou se composer de sous-ensembles de données de différentes origines, ou encore être dupliquées et donc disponibles en plusieurs endroits en même temps ; une personne peut se trouver « en mode itinérant » lorsque des données sont consultées ou interceptées. Dans le contexte de l'informatique décentralisée, le cas le plus fréquent semble être que les usagers ignorent où leurs données se trouvent à tel ou tel instant.

263 S'il est impossible de rattacher clairement des données à un lieu ou à un territoire, il devient problématique de s'appuyer sur le principe de territorialité pour définir les autorités compétentes pour perquisitionner ou saisir des preuves électroniques. Il a donc été proposé de dépasser le principe de territorialité. Le facteur juridique offrant une alternative à la territorialité pourrait être le « pouvoir d'utilisation ». Même si l'emplacement des données ne peut être clairement déterminé, les données peuvent être reliées à une personne qui a le pouvoir de « modifier, effacer, supprimer ou rendre inutilisables les données, ainsi que le droit d'en interdire l'accès à autrui ou d'en faire toute autre utilisation ».

264 Il a été suggéré que si l'emplacement des données n'est pas connu, mais que la personne ayant le pouvoir de les utiliser est physiquement présente sur le territoire de l'Etat enquêteur ou a la

---

[101] Non souligné dans le texte de la Convention

[102] Certains avancent que l'élargissement de la perquisition pourrait aussi couvrir des situations comparables au « droit de poursuite ». Au sein de l'Union européenne, les « poursuites » physiques sont possibles sans considération de frontières entre les Etats membres de l'espace Schengen, pour une série d'infractions graves.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:239:0001:0473:FR:PDF

[103] Spoenle, Jan (2010) : « Cloud computing and cybercrime investigations: territoriality vs the power of disposal », analyse, Projet sur la cybercriminalité, Conseil de l'Europe, Strasbourg.
Voir aussi Samson, Gareth (2008) sur le problème du « lieu » dans le cyberespace.

nationalité de cet Etat, les autorités répressives de l'Etat enquêteur pouvaient être autorisées à perquisitionner les données ou à y accéder.

265 Cependant, plusieurs garanties devraient être définies et des critères spécifiques devraient s'appliquer. Il a également été proposé de limiter un tel accès aux scénarios dans lesquels les moyens d'accès ont été légalement obtenus par les autorités répressives de l'Etat enquêteur, évitant ainsi que ces autorités ne piratent des systèmes informatiques situés dans d'autres pays.

6 Solutions concernant le type d'instrument

266 Le Groupe sur l'accès transfrontalier a examiné plusieurs solutions quant au type d'instrument qui pourrait être élaboré. Il a aussi recueilli, via le Secrétariat, l'avis du Jurisconsulte du Conseil de l'Europe.

6.1 Solutions possibles

267 Les solutions suivantes pourraient être envisagées :

6.1.1 Modification de l'article 32b de la Convention de Budapest

268 Une telle modification s'appliquerait à toutes les Parties, présentes et à venir. Deux possibilités sont envisageables :

- une procédure d'amendement simplifiée, telle que celle prévue à l'article 44 de la Convention de Budapest :

  Article 44 – Amendements

  1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

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

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

  4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article sera communiqué aux Parties en vue de son acceptation.

  5 Tout amendement adopté conformément au paragraphe 3 du présent article entrera en vigueur le trentième jour après que toutes les Parties auront informé le Secrétaire Général qu'elles l'ont accepté.

- un Protocole d'amendement qui serait élaboré au sein du cadre institutionnel du Conseil de l'Europe et conformément à ses règles habituelles en matière d'élaboration de conventions. Ce Protocole n'entrerait en vigueur qu'après avoir été ratifié par toutes les Parties.

269 Les avantages seraient que tous les Parties seraient associées à la décision (puisqu'elles devraient toutes accepter l'amendement), que la Convention resterait cohérente puisque l'amendement s'appliquerait à toutes les Parties actuelles et à venir et que l'amendement, en s'imposant à toutes les Parties, serait source de sécurité juridique.

270 L'inconvénient serait qu'il n'aurait d'effet contraignant qu'une fois accepté par toutes les Parties, ce qui pourrait prendre plusieurs années.

6.1.2 Recommandation du Comité des Ministres

271 Le Statut du Conseil de l'Europe, à l'article 15, prévoit que le Comité des Ministres peut adresser des Recommandations aux Etats membres. Ces Recommandations sont des instruments juridiques non contraignants.

272 Les Etats non membres, mais Parties à la Convention de Budapest pourraient donc participer à l'élaboration d'une Recommandation concernant la Convention de Budapest, mais non à son adoption. D'autre part, des Etats membres n'ayant pas ratifié la Convention participeraient à cette décision.

273 Une Recommandation pourrait s'avérer appropriée si elle proposait des solutions à des problèmes communs à tous les Etats membres, indépendamment de la Convention de Budapest sur la cybercriminalité.

274 Cependant, si elle couvrait des problèmes spécifiquement liés à la Convention de Budapest, elle ne serait pas appropriée :

- les Recommandations du Comité des Ministres ne sont adressées qu'aux Etats membres, ce qui exclurait certaines Parties à la Convention (les Etats non membres ne la recevraient que pour information) ;
- les Parties non membres du Conseil de l'Europe ne participeraient pas à l'adoption de la Recommandation par le Comité des Ministres ;
- on peut se demander pourquoi le Comité des Ministres devrait, par le biais d'une Recommandation, assurer le suivi d'un texte comme la Convention de Budapest alors que cela ne fait pas partie de ses attributions.

6.1.3 Protocole additionnel à la Convention de Budapest

275 Un Protocole additionnel pourrait être envisagé s'il visait à adopter des mesures allant au-delà de celles déjà prévues dans la Convention actuelle et dans son Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe (STCE n° 189), et s'il n'était pas obligatoire que toutes les Parties acceptent ce Protocole en le ratifiant ou en y adhérant. Il pourrait entrer en vigueur après qu'un certain nombre de Parties l'ont accepté (comme pour le Protocole STCE n° 189).

276 Un Protocole additionnel permettrait une certaine souplesse et une entrée en vigueur relativement rapide. En revanche, il ne s'imposerait qu'aux Parties qui l'ont accepté et pourrait donc diminuer la cohérence du régime de la Convention de Budapest. La capacité d'un Protocole additionnel à répondre effectivement à la question de l'accès transfrontalier dépendrait de la teneur de ce Protocole.

6.1.4 Interprétation de la Convention

277 Le principe de base en droit international est que les Parties sont responsables de l'interprétation des traités auxquelles elles ont adhéré[104]. L'accord sur l'interprétation de dispositions spécifiques de la Convention devrait se faire au sein de la Concertation des Parties (article 46 de la Convention de Budapest), c'est-à-dire du Comité de la Convention sur la cybercriminalité.

[104] En vertu de l'article 45, le Comité européen pour les problèmes criminels (CDPC) est tenu informé de l'interprétation et les Parties peuvent également lui soumettre un différend.

278 Deux types d'instruments pourraient être prévus :

- un accord formel sur l'interprétation, conformément à l'article 31.3.a de la Convention de Vienne sur le droit des traités[105]. Cet accord devrait être officiellement adopté par toutes les Parties. Dans la pratique, la procédure serait comparable à celle d'un Protocole d'amendement (voir plus haut). Un amendement simplifié, en vertu de l'article 44, pourrait s'avérer plus indiqué qu'un accord sur l'interprétation ;

- le T-CY pourrait adopter des lignes directrices ou un texte du même type et les adresser aux Parties à la Convention de Budapest et à leurs services opérationnels, afin de faciliter l'application de certaines dispositions de la Convention. Cette pratique semble répandue au sein des Comités du Conseil de l'Europe. Des lignes directrices, cependant, ne s'imposent pas aux Etats parties. D'un autre côté, elles peuvent être efficaces si les Parties se font mutuellement confiance pour les appliquer.

6.2 Solutions à retenir

279 Aux yeux du Groupe sur l'accès transfrontalier, les solutions à retenir sont les suivantes :

- une Note d'orientation du T-CY expliquant plus en détail les possibilités d'accès transfrontalier aux données actuellement offertes par la Convention de Budapest. Cette Note d'orientation devrait être soigneusement étudiée par les membres du T-CY, si besoin en concertation avec des entités privées et d'autres parties prenantes, mais pourrait entrer en vigueur dans un délai assez court ;

- un Protocole sur les mesures supplémentaires jugées nécessaires compte tenu des pratiques déjà appliquées par plusieurs Etats, assorti de conditions et de garanties. Il faudra du temps pour négocier un tel Protocole et, surtout, pour le faire ratifier par suffisamment de Parties pour qu'il entre en vigueur.

280 Cette « double approche » aiderait à clarifier les questions d'accès transfrontalier à court terme tout en laissant la place à des solutions à long terme en vertu du droit international. Elle semble pertinente compte tenu des évolutions technologiques, de la complexité et de l'intensité croissantes de la criminalité transnationale passant par des systèmes informatiques ainsi que des pratiques divergentes de certains Etats, qui accèdent à des données à l'étranger en allant au-delà des possibilités prévues par la Convention de Budapest. Il conviendrait de tenir dûment compte des garanties en matière de droits de l'homme et de prééminence du droit, des droits et intérêts légitimes des individus et des tiers et des préoccupations juridiques et politiques des Etats.

[105] http://untreaty.un.org/ilc/texts/instruments/francais/traites/1_1_1969_francais.pdf

7 Résumé et conclusions

281 Le Comité de la Convention sur la cybercriminalité (T-CY) a créé lors de sa 6e réunion plénière, en novembre 2011, un « Sous-groupe ad hoc sur la compétence et l'accès transfrontalier aux données et flux de données » (ou « Groupe sur l'accès transfrontalier ») dont le mandat expire le 31 décembre 2012.

282 Le Groupe sur l'accès transfrontalier s'est vu confier la mission suivante :

> élaborer un instrument tel qu'un amendement à la Convention, un protocole ou une recommandation visant à mieux réglementer l'accès transfrontalier aux données et aux flux de données, ainsi que le recours aux mesures d'enquêtes transfrontalières sur Internet et les questions y afférentes, et soumettre cet instrument au Comité dans un rapport présentant ses conclusions.

283 Le Groupe sur l'accès transfrontalier devait examiner en particulier l'application de l'article 32b de la Convention, les pratiques actuelles en matière d'enquêtes transfrontalières et les défis que représentent pour ces enquêtes le droit international sur le ressort territorial et sur la souveraineté des Etats. Le présent rapport reflète les conclusions des travaux menés par le Groupe sur l'accès transfrontalier entre janvier et novembre 2012.

284 Le Groupe sur l'accès transfrontalier estime que deux solutions pourraient être retenues parallèlement, à savoir l'élaboration d'une Note d'orientation du T-CY sur l'article 32 et celle d'un Protocole additionnel sur l'accès aux données. Avant de poursuivre, le Groupe sur l'accès transfrontalier aurait besoin que le T-CY confirme en plénière que ces solutions méritent effectivement d'être retenues. Sous réserve de cette confirmation, il est proposé que le mandat du Groupe sur l'accès transfrontalier soit prolongé jusqu'au 31 décembre 2013.

285 Les conclusions du présent rapport peuvent être résumées comme suit :

7.1 Nécessité de l'accès transfrontalier

286 La place grandissant des TIC dans la société s'accompagne d'un accroissement des infractions visant les systèmes informatiques ou commises au moyen de systèmes informatiques. La cybercriminalité porte atteinte aux droits individuels ; les gouvernements ont donc l'obligation positive de protéger la société de ce type de criminalité, entre autres par des mesures de répression appropriées.

287 L'un des premiers objectifs des autorités répressives consiste à recueillir des preuves. Pour la cybercriminalité, mais aussi pour d'autres types d'infractions pénales, elles prennent la forme de preuves électroniques. Les preuves électroniques sont évanescentes et peuvent être stockées sur de multiples territoires. Bien que le principal moyen de recueillir des preuves électroniques stockées dans un autre Etat soit l'entraide judiciaire, l'accès unilatéral aux données peut s'avérer nécessaire dans certaines situations.

288 La question de l'accès unilatéral, par les autorités répressives d'un Etat, à des données stockées sur un système informatique à l'étranger sans passer par l'entraide judiciaire est débattue depuis les années 1980. Elle est considérée comme urgente depuis le milieu des années 1990. Avec les Principes du G8 sur « l'accès transfrontalier à des données informatiques sans entraide judiciaire », adoptés par les ministres de l'Intérieur et de la Justice à Moscou en 1999, et l'adoption en 2001 de l'article 32 de la Convention de Budapest sur la cybercriminalité, très similaire, un accord a été trouvé sur l'accès transfrontalier dans des circonstances très limitées.

289 Ces dernières années, l'accès transfrontalier est devenu une nécessité de plus en plus impérieuse, compte tenu des points suivants :

- le nombre, la complexité et l'impact des actes de cybercriminalité transnationaux ;
- l'importance de plus en plus grande des preuves électroniques pour tous les types d'infractions pénales ;
- le volume des données et des équipements en circulation, la diversité des services offerts et le nombre de criminels et de victimes sur de multiples territoires ;
- le caractère de plus en plus évanescent des données et des preuves électroniques ;
- le recours à l'informatique décentralisée et aux services en ligne ;
- la « disparition du lieu », c'est-à-dire la difficulté à rattacher des données – et donc des preuves électroniques – à un territoire ou à un champ de compétence spécifique.

7.2 Préoccupations

290 Si les possibilités d'accès transfrontalier devaient s'accroître, il faudrait répondre à plusieurs préoccupations, dont les suivantes :

- des préoccupations juridiques et politiques pour les Etats, notamment concernant le principe de double incrimination ou le refus de coopérer si cela s'avère contraire à leur ordre interne. Ces principes sont pris en compte dans les mécanismes d'entraide judiciaire, mais non nécessairement dans les situations d'accès transfrontalier unilatéral ;
- la nécessité de garanties procédurales protégeant les droits des individus dans l'Etat où l'enquête se déroule. Les droits individuels doivent aussi être protégés dans les situations d'accès transfrontalier ;
- les conséquences pour les tiers, notamment les prestataires de services, qui peuvent recevoir des demandes contradictoires de la part de différents Etats ;
- des risques pour la protection des données personnelles. Les prestataires de services et autres entités du secteur privé peuvent enfreindre les règles de protection des données d'un Etat en divulguant des données aux autorités d'un autre Etat[106] ;
- des risques pour les opérations de police et pour les procédures judiciaires, que l'accès transfrontalier peut venir compromettre.

291 Par conséquent, afin que les Parties se fassent suffisamment confiance pour s'accorder sur un renforcement de l'accès transfrontalier, ce renforcement devrait s'accompagner de garanties et de procédures visant à protéger les droits des individus et des tiers et les intérêts légitimes des autres Etats. Des conditions doivent être mises en place pour empêcher une utilisation abusive de ces pouvoirs.

7.3 Dispositions actuelles de la Convention de Budapest

292 En vertu de la Convention de Budapest, le principal moyen d'obtenir des preuves électroniques stockées à l'étranger est l'entraide judiciaire, ou plus précisément une combinaison de mesures provisoires visant à conserver les preuves avant qu'elles ne disparaissent (articles 29 et 30 sur la

[106] Il convient de noter que les règles de protection des données sont en cours de modification au sein du Conseil de l'Europe et de l'Union européenne. Les travaux à venir sur l'accès transfrontalier devront tenir compte de ces modifications.

conservation rapide, article 35 sur le Réseau 24/7) et de demandes formelles de production de ces preuves (en particulier en vertu de l'article 31[107]).

293 L'article 32 est la disposition la plus pertinente concernant l'accès transfrontalier unilatéral. L'accès transfrontalier à des données publiques (article 32a) peut être considéré comme une pratique reconnue sur le plan international, élément du droit coutumier international même au-delà des Parties à la Convention de Budapest.

294 L'article 32b énonce une exception au principe de territorialité en autorisant l'accès transfrontalier unilatéral sans passer par l'entraide judiciaire dans des circonstances limitées. Cette disposition a été formulée de manière à pouvoir englober des scénarios complexes et différents. Elle se limite aux données situées dans des systèmes sur le territoire d'une Partie.

295 Le Groupe sur l'accès transfrontalier ne juge pas nécessaire de modifier l'article 32 sous sa forme actuelle. Cependant, cette disposition étant souvent mal comprise, le T-CY pourrait donner des orientations supplémentaires aux Parties sur des questions comme le sens à donner au « consentement », les lois qui s'appliquent pour définir le « consentement légal » et la personne « légalement autorisée », la personne habilitée à donner accès aux données ou à les divulguer ou le lieu où cette personne est supposée se trouver.

296 L'article 19.2 (perquisition et saisie) permet aux autorités répressives d'étendre un accès ou une perquisition légale du système initial à un système qui lui est connecté, si elles ont des raisons de penser que les données recherchées sont stockées dans un autre système sur leur territoire. Bien que cette mesure ait été conçue comme nationale dans le cadre de la Convention de Budapest, dans le contexte de l'informatique décentralisée, il est souvent difficile de savoir si le système connecté se trouve ou non sur le territoire des autorités répressives. En pratique, il semblerait que la mesure soit donc fréquemment appliquée sans restriction territoriale.

297 L'article 22 établit des principes de compétence généraux et assez larges. La territorialité est le premier principe, mais les principes de pavillon et de nationalité sont également mentionnés et la Convention de Budapest « n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne » (article 22.4). Il semblerait donc que l'article 22 ne constitue pas un obstacle à des solutions supplémentaires.

298 Même si le principe de territorialité restera prédominant, en particulier concernant la compétence qui s'exerce, on peut douter de la possibilité de l'appliquer dans le « cyberespace », fait de données voyageuses, fragmentées, composites ou dupliquées sur plusieurs serveurs relevant de divers ressorts territoriaux. Il n'est pas possible d'appliquer le principe de territorialité en l'absence de certitude quant à l'emplacement des données.

299 L'article 32 formule une exception au principe de territorialité puisqu'il prévoit l'exercice d'une compétence sur un territoire étranger, c'est-à-dire l'accès à des données qui sont techniquement stockées sur le territoire d'une autre Partie.

300 Les auteurs de la Convention de Budapest ne considéraient pas l'article 32 comme une panacée, jugeant que les situations non prévues par cet article n'étaient « ni autorisées ni exclues » et que des solutions supplémentaires pouvaient être adoptées à une étape ultérieure[108].

[107] Il semble que le potentiel de ces dispositions n'ait pas encore été pleinement exploité. Le T-CY, en novembre 2011, a décidé d'évaluer la mise en œuvre des articles 16, 17, 29 et 30 (sur la conservation rapide) en 2012, et d'entreprendre en 2013 une évaluation des dispositions en matière de coopération internationale (en particulier l'article 31).

7.4 Pratiques[109]

301 Les informations disponibles suggèrent que les autorités répressives accèdent de plus en plus à des données stockées dans des ordinateurs à l'étranger pour trouver des preuves électroniques. Ces pratiques peuvent aller au-delà des possibilités restreintes prévues à l'article 32b (accès transfrontalier avec consentement) et dans la Convention de Budapest en général.

- L'article 32b n'est pas très souvent utilisé par les autorités répressives pour accéder à des données stockées dans une autre Partie. Il est peut-être utilisé plus fréquemment pour consulter ou demander des données en possession de prestataires de services ou d'autres entités du secteur privé, telles que des données de trafic ou d'inscription, mais généralement pas des données de contenu générées par des usagers ou des clients. Il n'est pas toujours facile de savoir si une telle mesure est considérée comme une mesure transfrontalière au sens de l'article 32b ou comme une demande nationale, si l'entité en question fournit un service dans le pays des autorités en charge de l'enquête.

- Les autorités répressives peuvent aussi accéder directement à des données en élargissant une perquisition légale d'un système initial à un système qui lui est connecté. D'une certaine manière, l'article 19.2 est appliqué sans restriction au territoire des enquêteurs.

- Souvent, l'accès transfrontalier n'est pas délibéré. Les autorités répressives peuvent agir de bonne foi et ignorer ou ne pas avoir la certitude qu'elles perquisitionnent des données stockées sur un système à l'étranger ; il peut arriver aussi qu'elles ignorent de quel ressort territorial les données relèvent exactement.

- Dans certains Etats et en fonction de la situation précise, une fois que les autorités répressives savent que les données recherchées sont stockées à l'étranger, elles doivent interrompre les recherches, ne sont autorisées qu'à conserver une copie des données ou doivent en avertir l'autre Etat.

- Dans les Etats qui autorisent l'accès transfrontalier, seules les techniques d'enquête les moins intrusives sont permises, telles que l'accès avec consentement ou au moyen de données d'inscription obtenues légalement ou la conservation d'une copie des preuves, tandis que les techniques plus intrusives comme le piratage d'un compte ou d'un système, l'installation d'enregistreurs de frappe permettant une surveillance continue, la suppression de données ou la désactivation d'un système peuvent être interdites ou uniquement autorisées dans des circonstances limitées.

- De plus en plus, l'accès aux données stockées à l'étranger est obtenu via des prestataires de services ou d'autres entités du secteur privé, par consentement volontaire ou au travers de mandats judiciaires.

---

[108] Rapport explicatif de la Convention de Budapest, paragraphe 293.

[109] Le Groupe sur l'accès transfrontalier ne s'est intéressé qu'à l'accès aux données à des fins de justice pénale. Ces observations portent donc sur des enquêtes pénales et ne couvrent pas l'accès transfrontalier direct par les pouvoirs publics, ni l'accès à des données via des entités du secteur privé à des fins de renseignement ou de sûreté nationale.

- Les entités privées actives dans plusieurs pays peuvent se heurter à des exigences contradictoires : en répondant à une demande légalement formulée par un Etat, elles peuvent violer les règles de protection de la vie privée ou d'autres législations d'un autre Etat.

- L'accès transfrontalier aux données et l'utilisation des preuves ainsi obtenues dans une procédure pénale sont habituellement soumis à des conditions et garanties définies par l'Etat enquêteur.

302 Dans l'ensemble, les pratiques, les procédures et les conditions et garanties qui les accompagnent varient considérablement d'un Etat à l'autre. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données personnelles, la base juridique de l'accès aux données stockées à l'étranger ou « quelque part en ligne » ainsi que le principe de la souveraineté nationale.

7.5 Solutions proposées

7.5.1 Application plus efficace de la Convention de Budapest

303 La Convention de Budapest est un traité international qui reflète un accord entre les Parties sur les modalités de coopération entre elles. Elle est déjà en vigueur et le nombre de Parties est en augmentation. La Convention, sous sa forme actuelle, couvre une bonne part des besoins des autorités répressives en matière de cybercriminalité et de preuves électroniques. Elle permet aux gouvernements de respecter leur obligation positive de protéger les personnes et leurs droits. S'agissant de la coopération internationale, elle associe l'entraide judiciaire formelle à des mesures provisoires rapides visant à établir des preuves électroniques. Le potentiel de ce traité n'a pas encore été pleinement exploité par toutes les Parties.

304 Les Parties devraient utiliser efficacement la Convention de Budapest sur la cybercriminalité, et notamment ses dispositions en matière de coopération internationale. Les Parties sont invitées à prendre part aux évaluations de certains articles menées à bien par le Comité de la Convention sur la cybercriminalité (T-CY) et à donner suite aux recommandations formulées. Enfin, il serait souhaitable que davantage d'Etats adhèrent à la Convention de Budapest.

7.5.2 Note d'orientation du T-CY sur l'article 32

305 Le T-CY devrait préparer une Note d'orientation sur l'article 32b afin d'aider les Parties à appliquer la Convention de Budapest, de corriger les malentendus concernant l'accès transfrontalier en vertu de cette Convention et de rassurer les tiers.

306 L'article 32b suppose de plus en plus la coopération d'entités du secteur privé. Il sera donc nécessaire de consulter des entités privées et des experts de la protection des données au cours de l'élaboration de la Note d'orientation.

7.5.3 Protocole additionnel sur l'accès aux preuves électroniques

307 Même si la priorité devrait aller à l'application efficace de la Convention de Budapest sous sa forme actuelle, et bien qu'une Note d'orientation du T-CY représente un moyen pragmatique d'en faciliter la mise en œuvre, des mesures supplémentaires seraient peut-être à envisager, notamment pour tenir compte des cas où les données passent d'un territoire à l'autre ou sont stockées sur des territoires multiples ainsi que des cas où l'emplacement physique des données n'est pas connu. Ces mesures pourraient figurer dans un Protocole additionnel à la Convention de Budapest.

308 Ce Protocole additionnel pourrait couvrir des situations possibles entre Parties à travers différents instruments, comme par exemple :

- l'accès transfrontalier avec consentement, mais non limité aux données stockées dans une autre Partie ;
- l'accès transfrontalier sans consentement mais par des moyens obtenus légalement ;
- l'accès transfrontalier sans consentement de bonne foi ou dans des situations urgentes ou exceptionnelles ;
- l'extension des perquisitions sans restriction au territoire de l'Etat enquêteur ;
- le pouvoir d'utilisation comme critère de légalité des recherches.

309 Il sera essentiel de prévoir des garanties et des conditions pour protéger les droits individuels et éviter les abus.

310 Le fait que les autorités répressives de nombreux Etats procèdent déjà à des accès transfrontaliers aux données au-delà du champ de la Convention de Budapest, sur une base juridique incertaine, avec des risques pour les droits individuels de procédure et de protection de la vie privée et en soulevant des inquiétudes quant à la souveraineté nationale, justifierait qu'on s'engage dans le processus difficile de négociation d'un instrument juridique international contraignant. A l'inverse, en l'absence d'un tel instrument, les risques vont peut-être augmenter.

7.6 Prochaines étapes

311 Le T-CY a adopté le présent rapport lors de sa 8e réunion plénière (5-6 décembre 2012) et a décidé de le rendre public.

312 Il a été decidé de prolonger le mandat du Groupe sur l'accès transfrontalier jusqu'au 31 décembre 2013, avec les missions suivantes :

- préparer une Note d'orientation sur l'article 32 de la Convention de Budapest, y compris en consultant des entités du secteur privé. Un projet de texte devrait être préparé pour discussion lors de la 9e réunion plénière du T-CY, mi-2013, et des représentants du secteur privé pourraient être auditionnés à cette occasion. La Note d'orientation serait ensuite présentée pour adoption à la 10e réunion plénière, avant le 31 décembre 2013 ;

- soumettre à l'approbation du T-CY (procédure écrite), pour juin 2013, un projet de mandat par lequel le Comité des Ministres chargerait le T-CY de préparer un Protocole additionnel. Le Groupe devrait à ce stade fournir d'autres éléments concernant le contenu et le champ d'un tel Protocole[110] ;

- dans l'attente du mandat du Comité d'experts, préparer un premier projet de Protocole pour discussion lors de la 10e réunion plénière du T-CY, avant le 31 décembre 2013.

313 Le T-CY a décidé d'inviter le Japon à désigner un expert à joindre le Groupe sur l'accès transfrontalier et d'ouvrir le travail du Groupe aux représentants des autres Parties à la Convention

[110] Le projet de mandat serait ensuite soumis pour approbation au Comité des Ministres via le Comité européen pour les problèmes criminels (CDPC).

qui souhaiteraient participer aux réunions. Des experts extérieurs peuvent être invités au cas par cas.

---

8 Annexes

8.1 Note d'orientation du T-CY sur l'accès transfrontalier (article 32) : premiers éléments

[Introduction

[L'objectif de la présente Note est de fournir des orientations aux Parties à la Convention de Budapest sur la cybercriminalité sur l'application de l'article 32, consacré à l'accès transfrontalier aux données.

[Elle est le reflet d'une analyse partagée par tous les membres du T-CY.

[Les autres situations ne sont ni autorisées ni exclues.

[Article 32 de la Convention de Budapest

Texte de l'article :

> Article 32 - Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public.
>
> Une Partie peut, sans l'autorisation d'une autre Partie :
> a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou
> b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Extrait du Rapport explicatif :

> 293. La question de savoir quand une Partie est autorisée à accéder unilatéralement aux données informatiques stockées sur le territoire d'une autre Partie a été longuement examinée par les auteurs de la Convention. Ils ont passé en revue de façon détaillée les situations dans lesquelles il pourrait être acceptable que des Etats agissent de façon unilatérale et celles dans lesquelles tel n'est pas le cas. En définitive, les auteurs ont conclu qu'il n'était pas encore possible d'élaborer un régime global juridiquement contraignant applicable à ce domaine. C'était partiellement dû au fait que l'on ne dispose à ce jour d'aucun exemple concret ; cela tenait également au fait que l'on considérait que la meilleure façon de trancher la question était souvent liée aux circonstances de chaque cas d'espèce, ce qui ne permettait guère de formuler des règles générales. Les auteurs ont fini par décider de ne faire figurer dans l'article 32 de la Convention que les situations dans lesquelles l'action unilatérale était unanimement considérée comme admissible. Ils sont convenus de ne réglementer aucune autre situation tant que l'on n'aurait pas recueilli de nouvelles données et poursuivi la discussion de la question. A cet égard, le paragraphe 3 de l'article 39 dispose que les autres situations ne sont ni autorisées ni exclues.
>
> 294. L'article 32 (Accès transfrontalier à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public) traite de deux situations : d'abord celle dans laquelle les données en question sont accessibles au public, et ensuite celle dans laquelle la Partie a obtenu accès à ou

reçu des données situées en dehors de son territoire, au moyen d'un système informatique situé sur son territoire, et a obtenu le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. La question de savoir qui est la personne « légalement autorisée » pour communiquer des données peut varier en fonction des circonstances, la nature de la personne et du droit applicable concernés. Par exemple, le message électronique d'une personne peut être stocké dans un autre pays par un fournisseur de services ou une personne peut stocker délibérément des données dans un autre pays. Ces personnes peuvent récupérer les données et, pourvu qu'elles aient une autorité légale, elles peuvent les communiquer de leur propre gré aux agents chargés de l'application de la loi ou leur permettre d'accéder aux données, tel que prévu à l'article.

[Interprétation de l'article 32 par le T-CY

[S'agissant de l'article 32a (accès transfrontalier à des données informatiques publiquement disponibles ou « données ouvertes »), aucun problème particulier n'a été soulevé et il n'est pour l'instant pas nécessaire que le T-CY donne des orientations supplémentaires.

[S'agissant de l'article 32b (accès transfrontalier avec consentement), le T-CY partage l'analyse suivante :

[Concernant les notions de « frontière » et de « lieu »

[L'accès transfrontalier consiste à « accéder unilatéralement [c'est-à-dire sans passer par l'entraide judiciaire] aux données informatiques stockées sur le territoire d'une autre Partie[111] ».

[Cette mesure ne peut s'appliquer qu'entre Parties.

[L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat ». Cela signifie que l'article 32b peut être utilisé lorsqu'on sait où les données se trouvent.

[Etant donné que l'article 32b n'autorise pas, mais n'exclut pas non plus d'autres situations, lorsqu'on ignore que les données sont stockées dans une autre Partie ou lorsqu'on n'en a pas la certitude, les Etats peuvent être amenés à évaluer eux-mêmes la légitimité d'une perquisition ou d'un autre type d'accès à la lumière de leur droit interne, des principes applicables de droit international ou de considérations liées aux relations internationales.

[Concernant le « consentement »

[L'article 32b prévoit que le consentement doit être légal et volontaire, ce qui signifie que la personne qui fournit l'accès ou consent à divulguer les données ne doit avoir été ni contrainte ni dupée. Les éléments constitutifs du consentement doivent être définis par le droit interne de la Partie auquel le consentement s'adresse, c'est-à-dire de la Partie qui demande l'accès transfrontalier.

[Etant donné que l'article 32b porte sur l'accès transfrontalier à des fins de justice pénale, le consentement devrait être donné de façon expresse.

[Concernant le droit applicable

[111] Paragraphe 293 du Rapport explicatif de la Convention de Budapest.

[S'agissant du « consentement légal » et de la personne « légalement autorisée » à divulguer les données, « légal » désigne pour des raisons pratiques le droit de l'Etat enquêteur, puisque les autorités répressives agissent normalement sur la base du droit de leur propre pays. En cas d'accès transfrontalier urgent, il ne serait pas réaliste de demander aux enquêteurs de vérifier les règles applicables à l'utilisation des données dans l'autre Partie.

[Cependant, s'il est évident que la divulgation ou l'obtention de l'accès violerait les lois de l'autre Partie ou les règles en matière d'utilisation des données, les autorités répressives devraient s'abstenir de poursuivre l'accès transfrontalier.

[Concernant la personne autorisée à fournir l'accès ou à divulguer les données

[S'agissant de savoir « qui » est « légalement autorisé » à divulguer des données, la réponse peut varier en fonction des circonstances et des règles applicables.

[Il peut s'agir d'un particulier donnant accès à sa messagerie électronique ou à d'autres données qu'il a stockées à l'étranger.

[La personne fournissant l'accès peut aussi être un prestataire de services via Internet ou en ligne ou une autre entité privée détenant des données pour le compte d'un individu, par exemple si les conditions d'utilisation du service le permettent ou si le prestataire est devenu propriétaire des données ou a le pouvoir d'en disposer. Dans ce cas, pour se conformer à l'article 32b, le prestataire de services doit fournir l'accès légalement et volontairement, par exemple sans violer le droit à la vie privée ou d'autres droits. Par conséquent, ce n'est généralement possible que pour les données détenues par l'entité privée, comme les données de trafic, d'inscription ou les autres données relatives au réseau, alors qu'il ne serait pas possible de divulguer légalement et volontairement des contenus générés par les utilisateurs. Une injonction judiciaire de saisie ou de production des données ne serait pas couverte par l'article 32b.

[Concernant l'emplacement de la personne qui fournit l'accès ou divulgue les données

[Le scénario habituel est que la personne qui fournit l'accès est physiquement présente sur le territoire de la Partie requérante. Dans ce cas, cette personne relève du ressort et des lois de l'Etat enquêteur.

[Cependant, de multiples situations sont possibles. On peut imaginer que la personne physique ou morale se trouve sur le territoire des autorités répressives requérantes lorsqu'elle consent à divulguer les données ou lorsqu'elle y donne effectivement accès, ou uniquement lorsqu'elle consent mais non lorsqu'elle donne l'accès, ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle consent à divulguer les données et/ou y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle consent à coopérer ou lorsqu'elle fournit effectivement l'accès. S'il s'agit d'une personne morale (comme une entité privée), elle peut être représentée sur le territoire de l'autorité répressive requérante, sur le territoire où se trouvent les données, voire en même temps dans un pays tiers.

[Il faut tenir compte du fait que beaucoup de Parties s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des autorités répressives étrangères recherchant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale.

[Considérations et garanties générales

[L'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques, au sens de l'article 14[112].

[Les Parties à la Convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de la prééminence du droit, conformément à l'article 15 de la Convention de Budapest. Les mesures doivent être appliquées en tenant compte des droits individuels et des intérêts des tiers.

[Les mesures ne peuvent être utilisées pour encourager la violation de lois dans l'Etat visé par les recherches.

[L'Etat perquisitionneur devrait envisager d'avertir l'Etat perquisitionné, si son droit national autorise une telle notification et si les données révèlent une infraction pénale ou semblent présenter un intérêt pour l'Etat perquisitionné.

[….]

[112] Article 14 – Portée d'application des mesures du droit de procédure
1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :
a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;
b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et
c à la collecte des preuves électroniques de toute infraction pénale.
3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.
b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :
i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et
ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé, cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

8.2 Mandat du GroupeGroupe ad hoc du T-CY sur l'accès transfrontalier aux données et sur les questions de compétence territoriale[113]

Le Comité de la Convention Cybercriminalité,

tenant compte

a. de l'article 46 (1) a) et c) de la Convention sur la cybercriminalité (STE n° 185) ;
b. de la décision, prise lors de la cinquième réunion du Comité Convention Cybercriminalité, «de charger le Bureau d'élaborer le mandat pour ses futures activités normatives sur la compétence et l'accès transfrontalier aux données et de le soumettre au Comité assorti d'une feuille de route pour sa mise en oeuvre dès que possible ».

et eu égard aux considérations suivantes :

a. depuis vingt-cinq années, qui comprennent donc la décennie qui a suivi l'avènement de la Convention sur la cybercriminalité, les technologies de l'information et de la communication, et notamment le rôle joué par Internet dans nos sociétés ont connu des changements spectaculaires. Nous sommes passés d'un monde réel vers un monde virtuel, ou numérique, qui par nature ne connaît pas de frontières. Le développement des TIC apporte beaucoup d'innovations louables ; revers de la médaille, le monde virtuel est également devenu très attrayant pour les délinquants. Généralement parlant, on est passé d'une criminalité traditionnelle assistée par l'informatique à une criminalité de haute technologie, émanant des TIC et visant les TIC. Internet offre aux criminels un important degré d'anonymité. Internet permet aux délinquants de cibler des victimes potentielles depuis n'importe quel point du monde, ce qui facilite grandement la victimisation de masse. En corrompant le système d'un fournisseur d'accès Internet qui gère des données pour des tiers, on touche une masse de données, puis les ordinateurs des usagers lorsqu'ils se connectent ;

b. De plus en plus d'informations électroniques sont stockées ailleurs que là où réside le suspect ou que se trouve son ordinateur. Très souvent, l'emplacement exact de données informatiques dématérialisées n'est pas connu des autorités enquêtant officiellement sur des infractions ou même de l'utilisateur. Uneévolution vers le « cloud computing » ou l'infonuagique entrave la sécurisation des preuves électroniques ou une poursuite et un jugement rapides des délinquants.

c. L'une des grandes questions à régler consiste à trouver un équilibre satisfaisant entre la confidentialité, la protection des données et d'autres droits fondamentaux d'une part, et la liberté d'action des organismes d'application de la loi d'autre part, qui puisse permettre aux autorités compétentes de remplir leurs obligations en mantière de protection des usagers ;

d. d. Bien que le cyberespace lui-même n'ait pas de frontières, les organismes d'application de la loi sont en général liés à une jurdiction spécifique ;
Parallèlement, la coopération transfrontalière s'avère indispensable et a déjà lieu dans bein des cas. il importe cependant de développer des règles plus précises quant à ce qui est autorisé dans chaque ressort territorial et ce qui ne l'est pas, afin de favoriser la coopération transfrontalière ;

e. Le texte actuel de l'article 32 de la Convention sur la cybercriminalité est le résultat d'un compromis adopté en 2001. A cette époque, le manque d'expérience concrète au niveau international concernant les situations transfrontalières citées plus haut, a empêché les règles générales d'aller plus loin que l'article 32b. L'énoncé du paragraphe 293 du rapport explicatif

[113] Approuvé par le T-CY lors de sa 6ème Réunion Plénière, 23-24 novembre 2011

exprime clairement que l'article 32 doit être compris comme un texte succinct approuvé par l'ensemble des parties à l'époque. Le rapport explicatif autorise les pays à aller au-delà de cette article : « les autres situations [que celles mentionnées à l'article 32] ne sont ni autorisées ni exclues ». L'article 39.3 de la Convention stipule : « Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie »;

f. Trouver un accord sur de nouvelles procédures assurant aux organismes d'application de la loi des pouvoirs d'enquête transfrontaliers plus directs et qui respecte les conditions et dispositifs de sécurité nécessaires est un défi majeur, mais le Comité de la Convention sur la Cybercriminalité est préparé à le relever.

Décide

a. de créer un groupe ad hoc, composé d'une partie de ses membres, qui examinera les questions suivantes :

   i. l'application de l'article 32 b) de la Convention sur la cybercriminalité ;
   ii. l'utilisation de mesures d'enquête transfrontalières sur Internet ;
   iii. les défis que représentent, pour les enquêtes transfrontalières sur Internet, le droit international applicable concernant le ressort territorial et la souveraineté de l'État ;

b. de charger le groupe ad hoc d'élaborer un instrument tel qu'un amendement à la Convention, un protocole ou une recommandation visant à mieux réglementer l'accès transfrontalier aux données et aux flux de données, ainsi que le recours aux mesures d'enquêtes transfrontalières sur Internet et les questions y afférentes, et de soumettre cet instrument au Comité dans un rapport présentantses conclusions ;

c. de prier le groupe ad hoc de tenir compte du questionnaire déjà envoyé, des réponses au questionnaire et des débats tenus par le T-CY en plénière depuis 2009 ;

d. de lui demander de présenter un rapport lors de la deuxième réunion plénière tenue par le T-CY en 2012 ;

e. que le groupe ad hoc sera composé de dix membres du Comité au plus, dotés des connaissances nécessaires sur le sujet. Les dépenses seront remboursées dans la limite des moyens disponibles. Le groupe peut s'appuyer sur des expertises extérieures ;

f. fde proposer que Le Comité européen pour les problèmes criminels (CDPC) peut envoyer un représentant aux réunions du groupe ad hoc, sans droit de vote, et à la charge du poste budgétaire du Conseil de l'Europe correspondant ;

g. que Le Secrétariat sera assuré par le Conseil de l'Europe ;

h. que le présent mandat expirera le 31 décembre 2012.

8.3 Références

Groupe de travail article 29 sur la Protection des données (Union européenne) (2012): Avis 05/2012 sur l'informatique en nuage" (adopté le 1er juillet 2012)
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf

Brown, Ian/Korff, Douwe (2012): Digital Freedoms in International Law – Steps to Protect Human Rights Online (report prepared for the Global Network Initiative, GNI)
https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

Council of Europe / European Committee on Crime Problems (1990): Computer-related crime (Final report on Recommendation (R(89)9 of the Committee of Ministers)
http://www.oas.org/juridico/english/89-9&final%20Report.pdf

Council of Europe / European Committee on Crime Problems (1990): Extraterritorial criminal jurisdiction.

Council of Europe / Committee of Ministers (1995): Recommendation R(95)13 concerning problems of criminal procedural law connected with information technology"
http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp

Council of Europe / PC-OC Committee (2008): Replies on Mutual Legal Assistance in Computer-Related Cases / Réponses sur L'entraide judiciaire dans les affaires liées à l'informatique (PC-OC (2008) 08 rev)

Council of Europe / PC-OC Committee (2008) : Replies on Mutual Legal Assistance in Computer-Related Cases (Austria / France) / Réponses sur l'entraide judiciaire dans les affaires liées à l'informatique (Autriche / France) (Addendum to PC-OC (2008) 08 Rev)

Council of Europe / PC-OC Committee (2009): Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases (PC-OC (2009) 05)

Council of Europe / Project CyberCrime@IPA (2012): Article 15 – Conditions and Safeguards under the Budapest Convention on Cybercrime (Discussion paper with contributions by Henrik Kaspersen, Joseph Schwerha and Drazen Dragicevic)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2467_SafeguardsRep_v18_29mar12.pdf

Council of Europe / T-CY Committee (2010): Transborder access to stored computer data (discussion paper December 2010)

Council of Europe / T-CY Committee (2010): Replies of the state parties to the draft questionnaire on the need for direct transborder access to data and data flows where other measures are not adequate or fail (T-CY (2010) 01)

Council of Europe / T-CY Committee (2010): Answers to questionnaire on the need for direct transborder access to data flows where other measures are not adequate or fail (T-CY (2010) 01 Addendum

Council of Europe / T-CY Committee (2010): Direct transfrontier access to data and dataflows under international law (Fifth meeting, Paris, 24 - 25 June 2010) (T-CY (2010) 05 Confidential)

Council of Europe / T-CY Committee (2011): Ad hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows: Draft Terms of Reference (T-CY (2011) 5 E

Court of New York (USA): US District Judge of New York, Post-indictment Protective Order (Nov 2011), US *v.* John Doe

European Court of Human Rights (2012): Extra-territorial jurisdiction of ECHR Member States – Factsheet
http://www.echr.coe.int/NR/rdonlyres/DD99396C-3853-448C-AFB4-67240B1B48AE/0/FICHES_Juridiction_Extraterritoriale_EN.pdf

G8 Justice and Interior Ministerial (October 1999): Principles on Transborder Access to Stored Computer Data
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/24%208%20Principles%20on%20Transborder%20Access%20to%20Stored%20Computer%20Data_en.pdf

IGP (USA): In Important Case, RIPE-NCC seeks legal clarity on how it responds to foreign court orders (John Doe *v.* Bootnet)
http://blog.internetgovernance.org/blog/_archives/2011/11/23/4944811.html

International Chamber of Commerce (ICC Commission on the Digital Economy) (2012): Cross-border law enforcement to company data – current issues under data protection and privacy law. Policy Statement. Document No. 373/507 – (7 February 2012)
http://www.iccwbo.org/uploadedFiles/Law_enforcement_access_to_company_data_final_20March12.pdf

ISS World Americas (2011) : Cloud Lawful Interception and Data Retention, including Lawful Interception as a Service (LIaaS), Data Retention as a Service (DRaaS), Law Enforcement Monitoring Facility as a Service (LEMFaaS), by Tony Rutkowski, VP, Yaana Technology

Kaspersen, Henrik (2009): Cybercrime and internet jurisdiction (Discussion Paper prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079repInternetJurisdictionrik1a%20_Mar09.pdf

Kromann Reumert Publication (2012): Government Access to Information in "the Cloud".
http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf

Lakatos, Alex (2012): The USA Patriot Act and the Privacy of Data Stored in the Cloud.
http://www.mayerbrown.com/files/Publication/ce02dec6-f143-46ec-a0a3-53c06d770707/Presentation/PublicationAttachment/f56ea23a-7fd4-40bb-9b78-57e0787774dc/12057.PDF

Maxwell, Winston/Wolf, Christopher (2012): A Global Reality: Governmental Access to Data in the Cloud (Hogan Lovells White Paper, 23 May 2012)
http://www.hldataprotection.com/uploads/file/Hogan%20Lovells%20White%20Paper%20Government%20Access%20to%20Cloud%20Data%20Paper%20(1).pdf

Microsoft (2010): Building Confidence in the Cloud: A Proposal for Industry and Government Action for Europe to Reap the Benefits of Cloud Computing (Brad Smith, General Counsel)

Piragoff, Donald/Easson Larissa (1997), Department of Justice Canada: Computer-Related Investigations: Search And Seizure - Options Paper (Summit of the Eight, Senior Experts Group on Transnational Organized Crime (Lyon Group), Subgroup on High-Tech Crime)

Piragoff, Donald/Easson Larissa (1997a), Department of Justice Canada: Computer-Related Investigations: Search And Seizure - Options Paper (version prepared for Council of Europe Committee of Experts on Crime in Cyberspace (PC-CY(97)40), 24 September 1997.

Planken, Erik (2010): Cybercrime investigations and state sovereignty: Some thoughts on the way forward

Planken, Erik (2012): Preparatory paper for the first meeting of the ad hoc Working Group on transborder investigations in cybercrime

Poullet, Yves/ Van Gyseghem, Jean-Marc/ Gérard, Jacques/Gayrel, Claire/ Moiny, Jean-Philippe (2010): Cloud computing and its implications on data protection (Discussion paper prepared for the Council of Europe/Global Project on Cybercrime)
http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1c.pdf

Salt, Marcos (2012): Acceso trasfronterizo de datos almacenados en soportes informáticos en los países de America Latina (contribution to Council of Europe Octopus Conference 2012)

Sansom, Gareth (2008): Website Location: Cyberspace vs. Geographic Space (Draft: April 3, 2008)

Schwerha, Joseph (2010): Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers" (Discussion paper prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

Seitz, Nicolai (2004): Transborder Search: A new perspective in law enforcement? In: International Journal of Communications Law & Policy, Issue 9 – Special Issue on Cybercrime, Autumn 2004
http://www.ijclp.net/files/ijclp_web-doc_2-cy-2004.pdf

Sieber, Ulrich (2012): Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag. München.
Extract: http://www.beck-shop.de/fachbuch/leseprobe/Deutscher-Juristentag-djt-Straftaten-Strafverfolgung-Internet-9783406630729_1907201206155217_lp.pdf

Soukieh, Kim (University of NSW) (2011): Cybercrime – the shifting doctrine of jurisdiction (published in Canberra Law Review (2011) Vol. 10)
http://www.canberra.edu.au/faculties/law/attachments/pdf/the-canberra-law-review-articles/Kim-Soukieh-CLR-2011-Vol.-10.pdf

Spoenle, Jan (2010): Cloud computing and cybercrime investigations: territoriality vs the power of disposal. Strasbourg (report prepared for Council of Europe / Global Project on Cybercrime)
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf

Yaana Technologies LLC (2011): Elements of Cloud Lawful Interception and Retained Data (Anthony Rutkowski / LI(11)0028)