T-CY
CYBERCRIME CONVENTION COMMITTEE
COMITÉ DE LA CONVENTION CYBERCRIMINALITÉ

T-CY(2013)29rev

Strasbourg, France
8 décembre2014

NOTES D'ORIENTATION DU T-CY

Adoptées par le T-CY lors des 8e, 9e et 12e Réunions Plénières

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

A propos des notes d'orientation

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en oeuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies[1].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La Convention « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[2], et ce pour que de nouvelles formes de délits soient toujours couvertes par la Convention.

Contact

Alexander Seger
Secrétaire du Comité de la Convention Cybercriminalité (T-CY)
Direction Générale des Droits de l'Homme et de l'Etat de droit
Conseil de l'Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

[1] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[2] Paragraphe 36 du rapport explicatif.

Index

1 Note d'orientation sur la notion de « système 1informatique »

Introduction

Lors de sa première réunion à Strasbourg, les 20 et 21 mars 2006, le T-CY s'est penché sur la portée de l'expression « système informatique » telle qu'elle se trouve définie à l'article 1.a de la Convention de Budapest, compte tenu des nouvelles formes de technologie qui vont au-delà des simples ordinateurs de bureau ou ordinateurs centraux traditionnels.

Depuis 2004, date à laquelle la Convention a été rédigée, de nouveaux dispositifs sont apparus, avec notamment la génération moderne des téléphones portables dits « smartphones », les ordinateurs de poche (PDA), les tablettes et autres, qui permettent de produire, traiter ou transmettre des données. D'où la nécessité de voir si la notion de « système informatique » qu'utilise la Convention de Budapest couvre ces nouveaux dispositifs.

Le T-CY a décidé, en 2006, que les dispositifs en question étaient couverts par la définition du « système informatique » qui figure à l'article 1.a de la Convention.

La présente note d'orientation consacre cette interprétation commune des Parties, telle qu'elle ressort du rapport de la 1ère réunion (document T-CY(2006)11).

Article 1.a. de la Convention de Budapest sur la cybercriminalité (STCE n° 185)

Texte de la Convention

> **Article 1 –Définitions**
>
> Aux fins de la présente Convention,
>
> a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données

Extrait du Rapport explicative

> 23. Aux fins de la Convention, un système informatique est un dispositif composé de matériel et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau. « Automatisé » signifie sans intervention humaine directe, le « traitement des données » est un ensemble d'opérations appliquées à des données et effectuées par le biais de l'exécution d'un programme informatique. Un « programme informatique » est un ensemble d'instructions pouvant être exécutées par l'ordinateur pour obtenir le résultat attendu. Un ordinateur peut exécuter différents programmes. Dans un système informatique, on distingue généralement plusieurs composantes, à savoir le processeur ou l'unité centrale, et les périphériques. Par « périphérique », on entend un dispositif qui remplit certaines fonctions spécifiques en interaction avec l'unité centrale : imprimante, écran, lecteur/graveur de CD-ROM ou autre moyen de stockage, par exemple.
>
> 24. Un réseau est une interconnexion entre deux systèmes informatiques ou plus. Les connexions peuvent être reliées à la terre (fil ou câble, par exemple), sans fil (radio, infrarouge ou satellite, par exemple), ou les deux. Un réseau peut être géographiquement limité à une zone peu étendue (réseau local) ou couvrir une zone étendue (réseau étendu), et de tels réseaux peuvent eux-mêmes
> 5

être interconnectés. L'Internet est un réseau mondial composé de nombreux réseaux interconnectés, qui utilisent tous les mêmes protocoles. Il existe encore d'autres types de réseaux, connectés ou non à l'Internet, capables de faire circuler des données entre des systèmes informatiques. Les systèmes informatiques peuvent être connectés au réseau en tant que points de sortie ou comme moyen de faciliter la transmission de l'information (routeurs et dispositifs similaires, par exemple). L'important, c'est que les données soient échangées sur le réseau.

Déclaration du T-CY concernant la notion de « système informatique » (article 1.a. de la Convention de Budapest)

L'article 1.a de la Convention définit un « système informatique » comme « tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ».

Le T-CY considère que cette définition englobe, par exemple, les téléphones portables modernes, qui sont des appareils multifonctionnels capables de produire, traiter et transmettre des données, leurs multiples fonctions consistant notamment à accéder à l'Internet, à envoyer des courriers électroniques, à joindre et transmettre des fichiers, ainsi qu'à télécharger des contenus ou documents.

De même, le T-CY a conscience que les assistants numériques personnels (PDA), qu'ils soient ou non dotés de la fonctionnalité sans fil, peuvent eux aussi produire, traiter et transmettre des données.

Le T-CY souligne que, lorsque ces dispositifs exécutent de telles fonctions, ils traitent des « données informatiques » au sens de l'article 1.b. Il considère par ailleurs qu'ils génèrent aussi, ce faisant, des « données relatives au trafic » au sens de l'article 1.d.

Dès lors qu'ils traitent de telles données, les dispositifs en question se comportent comme un « système informatique » au sens de l'article 1.a.

Le T-CY estime qu'une telle acception est conforme à l'interprétation que donne du « système informatique » le rapport explicatif de la Convention et que cette dernière a vocation à couvrir ces dispositifs dans leur utilisation en tant que tel.

Conclusion

Le T-CY considère que la définition du « système informatique » qui figure à l'article 1.a couvre de nouvelles formes de technologie qui vont au-delà des simples ordinateurs de bureau ou ordinateurs centraux, avec notamment les téléphones portables modernes, les « smartphones », les assistants numériques personnels, les tablettes et autres appareils similaires.

2 Note d'orientation sur les dispositions de la Convention de 2Budapest visant les botnets[3]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'usage et la mise en oeuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies[4].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note traite de la question des botnets.

La Convention « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[5], et ce pour que de nouvelles formes de logiciels malveillants ou de délits soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux botnets.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE no 185)

Le terme « botnet » peut désigner :

> « un groupe d'ordinateurs qui ont été contaminés par des logiciels malveillants (virus informatiques). Un tel réseau d'ordinateurs compromis ("zombies") peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les "zombies" peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé "centre de commande et de contrôle" ».[6]

Des ordinateurs peuvent être reliés entre eux à des fins criminelles ou pour de bonnes causes[7]. Le fait que les botnets soient constitués d'ordinateurs reliés entre eux n'est donc pas un critère pertinent. L'élément essentiel est que les ordinateurs des botnets sont utilisés sans autorisation, à des fins criminelles et pour causer des dégâts majeurs.

Les botnets sont visés par certains articles de la Convention, en fonction de l'action précise qu'ils accomplissent. Ces articles sont énumérés ci-dessous. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.), dont la preuve devrait être apportée sans difficulté en présence de botnets.

---

[3] Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

[4] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[5] Paragraphe 36 du rapport explicatif.

[6] Proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre du Conseil 2005/222/JAI (COM (2010) 517 final).

[7] Des réseaux d'ordinateurs peuvent être sciemment créés à des fins criminelles. Les infractions commises par ces réseaux sont couvertes par la Convention, mais ne sont pas examinées dans la présente note.

Articles pertinents	Exemples
Article 2 – Accès illégal	La création et l'exploitation d'un botnet nécessitent un accès illégal à des systèmes informatiques[8]. Les botnets peuvent servir à accéder illégalement à d'autres systèmes informatiques.
Article 3 – Interception illégale	Les botnets peuvent utiliser des moyens techniques pour intercepter des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	La création d'un botnet altère toujours et peut endommager, effacer, dégrader ou supprimer des données informatiques. Les botnets eux-mêmes endommagent, effacent, dégradent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les botnets peuvent entraver le fonctionnement d'un système informatique, notamment au moyen d'attaques par déni de service distribué[9].
Article 6 – Abus de dispositifs	Les botnets sont tous des dispositifs relevant de la définition figurant à l'article 6, car ils sont conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5[10]. Les programmes utilisés pour créer et exploiter des botnets entrent aussi dans le champ de l'article 6. Par conséquent, l'article 6 érige en infractions pénales la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mises à disposition des dispositifs que sont les botnets ou les programmes utilisés pour leur création ou leur exploitation.
Article 7 – Falsification informatique	Selon la façon dont il a été conçu, le botnet peut introduire, altérer, effacer ou supprimer des données informatiques, engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques.
Article 8 – Fraude informatique	Les botnets peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 9 – Pornographie enfantine	Les botnets peuvent diffuser des contenus qui relèvent de l'exploitation d'enfants.
Article 10 – Infringements related to copyrights and related rights	Les botnets peuvent diffuser illégalement des données qui sont protégées par les lois relatives à la propriété intellectuelle.

[8] Voir également la note d'orientation no 1 relative à la notion de « système informatique ».

[9] Voir la note d'orientation sur ce sujet

[10] Les Parties qui émettent des réserves concernant l'article 6 doivent néanmoins toujours ériger en infraction pénale la vente, la diffusion ou la mise à disposition de dispositifs visés par ledit article.

Article 10 – Atteinte à la propriété intellectuelle et aux droits connexes	Les botnets peuvent diffuser illégalement des données qui sont protégées par les lois relatives à la propriété intellectuelle.
Article 11 – Tentative et complicité	Les botnets peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complice de leur commission.
Article 13 – Sanctions	Les botnets sont utilisés à de multiples fins criminelles, dont certaines ont une incidence grave sur les personnes, les institutions publiques ou privées ou les infrastructures essentielles. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux botnets soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux botnets « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les botnets portent atteinte à un nombre important de systèmes ou que les attaques causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

Déclaration du T-CY

La liste des articles concernant les botnets présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen des botnets et les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que les botnets, sous leurs différents aspects, sont couverts par la Convention de Budapest.

3 Note d'orientation sur les attaques DDOS[11]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en oeuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies[12].

Les notes d'orientation reflètent la vision commune de toutes les Parties quant à l'utilisation de la Convention.

La présente note est consacrée à la question des attaques par déni de service (DOS) et par déni de service distribué (DDOS).

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »13[13], et ce pour que les nouvelles formes de logiciels malveillants ou d'infractions soient toujours couvertes par la Convention.

La présente note montre dans quelle mesure plusieurs articles de la Convention s'appliquent aux attaques DOS et DDOS.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE n° 185)

Les attaques DOS visent à rendre un système informatique indisponible pour ses utilisateurs par divers moyens, dont la saturation des ordinateurs ou réseaux ciblés par des demandes de communication externes, qui ralentit l'accès au service pour les utilisateurs légitimes. Les attaques DDOS sont des attaques par déni de service exécutées par plusieurs ordinateurs en même temps. Il existe actuellement plusieurs manières de lancer des attaques DOS et DDOS, par exemple envoyer des requêtes incorrectes à un système informatique, dépasser le nombre maximal d'utilisateurs ou envoyer un nombre de courriers électroniques supérieur à celui que le serveur peut recevoir et traiter.

Les attaques DOS et DDOS sont visées par certains articles de la Convention, en fonction de ce qu'elles accomplissent. Ces articles sont énumérés ci-dessous. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.), dont la preuve devrait être apportée sans difficulté en cas d'attaque DOS ou DDOS.

Interprétation par le T-CY de la criminalisation des attaques DDOS

Articles pertinents	Exemples
Article 2 – Accès illégal	Par le biais des attaques DOS et DDOS il est possible d'accéder à un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les attaques DOS et DDOS peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Une attaque DOS ou DDOS vise précisément à entraver gravement le fonctionnement d'un système informatique.

[11] Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

[12] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[13] Paragraphe 36 du rapport explicatif.

Article 11 – Tentative et complicité	Les attaques DOS et DDOS peuvent être utilisées pour tenter de commettre plusieurs des infractions spécifiées dans la Convention ou pour se rendre complice de leur commission (telles que la falsification informatique, article 7 ; la fraude informatique, article 8 ; les infractions se rapportant à la pornographie enfantine, article 9, et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes, article 10).
Article 13 – Sanctions et mesures	Les attaques DOS et DDOS peuvent être dangereuses de multiples façons, en particulier lorsqu'elles sont dirigées contre des systèmes qui sont essentiels au quotidien – par exemple, si un système bancaire ou hospitalier est rendu indisponible. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des infractions liées aux attaques DOS et DDOS soit trop clémente et ne permette pas la prise en considération de circonstances aggravantes, de la tentative ou de la complicité. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux attaques DOS et DDOS « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques DOS ou DDOS portent atteinte à un nombre important de systèmes ou causent des dégâts majeurs, y compris des décès, des blessures physiques ou l'endommagement d'infrastructures essentielles.

Déclaration du T-CY

La liste des articles concernant les attaques DOS et DDOS présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY estime que les différents aspects de ces attaques sont couverts par la Convention de Budapest.

4 Note d'orientation sur la Fraude par usurpation d'identité et hameçonnage[14]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en oeuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies[15].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question de la fraude par usurpation d'identité et hameçonnage (« phishing ») ou par des pratiques analogues[16].

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »13[17], et ce pour que les nouvelles formes de logiciels malveillants ou d'infractions soient toujours couvertes par la Convention.

Cette note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent à l'usurpation d'identité par voie informatique en lien avec la fraude.

Identity theft and phishing

Il n'existe pas de définition universellement acceptée de ce qui constitue une usurpation d'identité. Malgré le caractère fluctuant de l'usage de cette notion, on entend communément par « usurpation d'identité » des infractions pénales qui consistent à obtenir et à utiliser de façon frauduleuse (à son insu et sans son consentement) les données personnelles d'une autre personne. Le terme « fraude à l'identité » est parfois employé comme synonyme, bien que cette notion englobe également le fait d'utiliser une fausse identité, qui n'est pas forcément réelle.

Les renseignements personnels d'une personne réelle ou fictive peuvent être utilisés à mauvais escient pour commettre de nombreux actes illicites. La présente note d'orientation ne traite cependant que des usurpations d'identité liées à la fraude.

Cela peut impliquer l'appropriation frauduleuse d'informations relatives à l'identité (par exemple nom, date de naissance, adresse actuelle ou adresses antérieures) d'une autre personne, à son insu et sans son consentement. Ces renseignements personnels sont ensuite utilisés pour obtenir des biens et services en son nom.

Ce type d'agissements peut prendre plusieurs formes comme le « phishing », le « pharming », le « spear phishing », le « spoofing » ou toute autre conduite analogue visant, par exemple, à obtenir un mot de passe ou d'autres clés d'accès, souvent par le biais de courriers électroniques ou de sites web falsifiés.

---

[14] Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

[15] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[16] Ces pratiques sont connues sous des appellations diverses : spear phishing ou « harponnage », SMiShing, pharming et vishing.

[17] Paragraphe 36 du rapport explicatif.

L'usurpation d'identité est un véritable fléau qui touche les gouvernements, les entreprises et les citoyens. Ce phénomène mine la confiance dans les technologies de l'information.

La plupart des systèmes juridiques ne prévoient pas de délit spécifique d'usurpation d'identité. Les auteurs d'usurpation d'identité sont normalement inculpés de délits plus graves (comme la fraude financière). L'obtention d'une fausse identité implique normalement la commission d'une infraction, comme la falsification de documents ou l'altération de données informatiques. Une fausse identité facilite la perpétration de nombreux crimes dont l'immigration illégale, la traite des êtres humains, le blanchiment d'argent, le trafic de drogue et la fraude financière contre les gouvernements et le secteur privé, mais est généralement associée à la fraude.

Sur le plan conceptuel, une usurpation d'identité peut se décomposer en trois étapes :

- Phase 1 – L'obtention des renseignements personnels par des moyens divers tels que le vol physique, l'utilisation de moteurs de recherche, des attaques de l'intérieur ou de l'extérieur (accès illicite aux systèmes informatiques, Trojans, « keyloggers », logiciels espions et autres programmes malveillants), ou bien par le recours au hameçonnage ou à d'autres techniques d'ingénierie sociale.
- Phase 2 – La possession et la cession des renseignements personnels (par exemple, la vente de ces informations à des tiers).
- Phase 3 – L'utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions, par exemple en prenant l'identité d'une autre personne pour exploiter des comptes en banque ou des cartes de crédit, ouvrir de nouveaux comptes, contracter des prêts et crédits, commander des biens et services ou diffuser des programmes malveillants.

En conclusion : l'usurpation d'identité (y compris le hameçonnage et les conduites analogues) sert généralement à la préparation de nouveaux agissements criminels, comme la fraude informatique. Bien que l'usurpation d'identité ne constitue pas une infraction en elle-même, les services chargés de l'application des lois peuvent engager des poursuites pour les infractions connexes.

Interprétation de la pénalisation de la fraude par usurpation d'identité donnée par le T-CY au regard de la Convention de Budapest

La Convention de Budapest traite avant tout des actes criminels et n'aborde pas expressément les techniques ou technologies employées. En conséquence, elle ne contient pas de dispositions spécifiques relatives à l'usurpation d'identité ou au hameçonnage. Cependant, la pleine application des dispositions de droit matériel de la Convention permet aux Etats d'ériger en infraction pénale tout agissement lié à une usurpation d'identité.

La Convention fait obligation aux Etats d'ériger en infraction pénale des agissements tels que l'accès illégal à un système informatique, l'interception illégale de données, l'atteinte à l'intégralité des données, l'atteinte à l'intégralité du système, l'abus de dispositifs et la falsification informatique :

Phases	**Articles de la Convention**	**Exemples**
Phase 1 – Obtention des renseignements personnels	Article 2 – Accès illégal	Lorsqu'un pirate contourne la protection par mot de passe, enregistre les frappes d'un clavier (« keylogging ») ou exploite les failles des logiciels, il est possible d'accéder illégalement à l'ordinateur à des fins d'usurpation d'identité ou de hameçonnage. L'accès illégal aux systèmes informatiques figure parmi

		les infractions les plus communément commises pour obtenir des données sensibles, comme les renseignements personnels.
	Article 3 – Interception illégale	L'usurpation d'identité comporte souvent le recours à des dispositifs de surveillance (« keyloggers ») ou autres types de programmes malveillants pour intercepter illégalement des transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système informatique contenant des données sensibles, comme les renseignements personnels.
	Article 4 – Atteinte à l'intégrité des données	L'usurpation d'identité ou le hameçonnage peuvent endommager, effacer, dégrader, altérer ou supprimer des données informatiques. Cela intervient souvent dans le cadre du processus d'obtention d'un accès illégal, moyennant l'installation d'un « keylogger » pour obtenir des données sensibles.
	Article 5 – Atteinte à l'intégrité du système	L'usurpation d'identité ou le hameçonnage peuvent entraver le fonctionnement d'un système informatique pour voler ou faciliter le vol de données à caractère personnel.
	Article 7 – Falsification informatique	L'usurpation d'identité ou le hameçonnage peuvent donner lieu à l'introduction, l'altération, l'effacement ou la suppression de données informatiques, engendrant des données non authentiques qui seront prises en compte ou utilisées à des fins légales comme si elles étaient authentiques. Le hameçonnage est probablement l'illustration la plus courante d'une falsification informatique (page web falsifiée d'un établissement financier par exemple). Cette activité illicite est par conséquent la méthode la plus couramment employée pour obtenir des données sensibles, comme les renseignements personnels.
Phase 2 – Possession et cession des renseignements personnels	Article 6 – Abus de dispositifs	Les données personnelles volées – mots de passe, clés d'accès, cartes de crédit et autres – peuvent être considérées comme la possession d'un « dispositif, y compris un système informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 » de la Convention ou « d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique ».

Phase 3 – Utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions	Article 8 – Fraude informatique	L'utilisation d'une identité frauduleuse pour introduire, altérer, effacer ou supprimer des données informatiques et/ou porter atteinte au fonctionnement d'un système informatique peut servir à exploiter des comptes en banque ou des cartes de crédit, à contracter des prêts et crédits ou commander de biens et services, et peut donc causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique.
Toutes les phases	Article 11 – Tentative et complicité	L'obtention, la possession et la cession de données personnelles peuvent constituer une tentative de commettre plusieurs des infractions spécifiées dans la Convention ou de se rendre complice de leur commission.
	Article 13 – Sanctions	L'usurpation d'identité sert à de multiples fins criminelles dont certaines ont une incidence grave sur les personnes et les institutions publiques ou privées. Il est cependant possible que la sanction prévue par la législation nationale de certaines Parties à l'égard de l'usurpation d'identité soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes. D'où, éventuellement, la nécessité pour ces Parties d'envisager la révision de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à l'usurpation d'identité « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si l'usurpation d'identité porte atteinte à un grand nombre de personnes ou cause un préjudice considérable ou expose une personne à un danger

Déclaration du T-CY

Le T-CY considère que ci-dessus sont illustrées l'étendue et les multiples éléments de pénalisation de l'usurpation d'identité et du hameçonnage ainsi que les dispositions pénales qui pourraient s'appliquer.

Par conséquent, le T-CY s'accorde à dire que ces infractions, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

5 Note d'orientation sur les attaques visant les infrastructures 5d'information critiques[18]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en oeuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies[19].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des attaques visant les infrastructures d'information critiques.

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[20], et ce pour que les nouvelles formes de logiciels malveillants ou d'infractions soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux attaques visant les infrastructures d'information critiques.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE n°185)

Les infrastructures critiques désignent en général les systèmes et les actifs, physiques ou virtuels, indispensables à la vie d'un pays et dont le mauvais usage, l'arrêt ou la destruction aurait un effet dévastateur sur la sécurité nationale et la défense, la sécurité économique, la santé ou la sûreté publiques ou n'importe quelle combinaison de ces éléments. La définition des infrastructures critiques varie selon les pays. Toutefois, pour de nombreux pays, les infrastructures critiques englobent l'énergie, l'alimentation, l'eau, les combustibles, les transports, les communications, les finances, l'industrie, la défense et les secteurs des services publics et du gouvernement.

Les infrastructures critiques sont souvent gérées par des systèmes informatiques, notamment ceux connus sous le nom de systèmes de contrôle industriels (SCI) ou de systèmes de télésurveillance et d'acquisition de données (SCADA). Ces systèmes sont généralement désignés sous le nom d'infrastructures d'information critiques.

Selon des sources privées et gouvernementales, un nombre important mais inconnu d'attaques visant des infrastructures d'information critiques se produit chaque année dans le monde entier. Ces attaques ont recours aux mêmes techniques que celles utilisées par la criminalité électronique. La différence réside dans l'impact de ces attaques sur la société : elles peuvent retirer des fonds du Trésor public, interrompre l'approvisionnement en eau, perturber le contrôle du trafic aérien, etc.

Les formes d'attaques des infrastructures d'information critiques, actuelles et futures, sont visées par les articles de la Convention figurant ci-dessous, en fonction de la nature de l'attaque. Chaque disposition

[18] Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

[19] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[20] Paragraphe 36 du rapport explicatif.

contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

Interprétation par le T-CY de l'incrimination des attaques visant des infrastructures d'information critiques

Articles pertinents	Exemples
Article 2 – Accès illégal	Les attaques contre les infrastructures d'information critiques peuvent s'introduire dans un système informatique.
Article 3 –Interception illégale	Les attaques contre les infrastructures d'information critiques peuvent utiliser des moyens techniques pour intercepter des transmissions non publiques de données informatiques, à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les attaques contre les infrastructures d'information critiques peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les attaques contre les infrastructures d'information critiques peuvent porter atteinte au fonctionnement d'un système informatique ; il pourrait en fait s'agir de leur objectif premier.
Article 7 – Falsification informatique	Les attaques contre les infrastructures d'information critiques peuvent introduire, altérer, effacer ou supprimer des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques.
Article 8 – Fraude informatique	Les attaques contre les infrastructures d'information critiques peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les attaques contre les infrastructures d'information critiques peuvent être utilisées pour tenter de commettre des infractions spécifiées dans le traité ou pour se rendre complices de leur commission.
Article 13 – Sanctions	Les incidences des attaques contre les infrastructures d'information critiques sont multiples (elles peuvent varier selon les pays pour des raisons techniques, culturelles ou autres) mais les pouvoirs publics s'y intéressent généralement lorsqu'elles entrainent des préjudices graves ou de grande ampleur. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques contre les infrastructures d'information critiques soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions

	pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques contre les infrastructures d'information critiques portent atteinte à un nombre important de systèmes ou provoquent des dégâts considérables, y compris des décès ou des blessures physiques.

Déclaration du T-CY

La liste des articles concernant les attaques contre les infrastructures d'information critiques présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY s'accorde à dire que ces attaques, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

6 Note d'orientation sur les nouvelles formes de logiciels malveillants[21]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé d'établir des notes d'orientation visant à faciliter l'utilisation et la mise en oeuvre effectives de la Convention de Budapest sur la cybercriminalité, compte tenu notamment des évolutions du droit, des politiques et des technologies[22].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des nouvelles formes de logiciels malveillants.

La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[23], et ce pour que les nouvelles formes de logiciels malveillants ou délits soient toujours couvertes par la Convention.

La présente note d'orientation montre dans quelle mesure différents articles de la Convention s'appliquent aux nouvelles formes de logiciels malveillants.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STCE n°185)

existe actuellement de nombreuses formes de logiciels malveillants. Selon l'Organisation de coopération et de développement économiques « le terme général de « logiciel malveillant » désigne un logiciel introduit dans un système d'information afin de causer des dommages à ce système ou à d'autres systèmes, ou de les destiner à une utilisation autre que celle voulue par leurs utilisateurs légitimes »24. Les formes les plus connues englobent les vers, les virus et les chevaux de Troie. Les logiciels malveillants, sous leurs formes actuelles, peuvent dérober des données en les copiant et en les envoyant vers une autre adresse ; manipuler des données ; porter atteinte au fonctionnement de systèmes informatiques, y compris ceux qui contrôlent des infrastructures critiques ; les « ransomware » peuvent effacer, supprimer ou bloquer l'accès à des données ; et des logiciels malveillants taillés sur mesure peuvent cibler des systèmes informatiques spécifiques.

Selon des sources privées et gouvernementales, de nouvelles formes de logiciels malveillants sont conçues et découvertes en grand nombre chaque année. Leurs objectifs sont variés. Tout comme les formes plus anciennes, les nouvelles formes de logiciels malveillants peuvent voler de l'argent, mettre hors service les systèmes d'approvisionnement en eau, menacer les utilisateurs etc.

Le nombre et la diversité des formes de logiciels malveillants sont tels qu'il serait impossible, même pour les formes connues actuellement, de les définir dans le cadre d'une loi pénale. La Convention sur la cybercriminalité évite délibérément l'utilisation de termes tels que virus, vers et chevaux de Troie. Dans la mesure où la tendance évolue aussi dans le domaine des logiciels malveillants, l'utilisation de ces termes dans la Convention la rendrait rapidement obsolète et contre-productive.

Il est également impossible, bien évidemment, de décrire les formes futures dans une loi.

---

[21] Adoptée lors de la 9ème réunion plénière du T-CY (4-5 juin 2013)

[22] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[23] Paragraphe 36 du rapport explicatif.

Pour ces raisons, il importe de se concentrer sur les objectifs et les effets des logiciels malveillants. Ces derniers sont déjà connus et peuvent être visés par une loi.

Par conséquent, les logiciels malveillants, que ce soit sous leur forme actuelle ou leur forme future, sont visés par les articles de la Convention figurant ci-dessous, en fonction de l'action précise qu'ils accomplissent. Chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse » etc.) dont les autorités devraient tenir compte au moment de qualifier un délit.

Interprétation par le T-CY de l'incrimination des nouvelles formes de logiciel malveillant

Articles pertinents	**Exemples**
Article 2 – Accès illégal	Les logiciels malveillants peuvent être utilisés pour s'introduire dans des systèmes informatiques.
Article 3 –Interception illégale	Les logiciels malveillants peuvent être utilisés pour intercepter des transmissions non publiques de données informatiques, à destination, en provenance ou à l'intérieur d'un système informatique.
Article 4 – Atteinte à l'intégrité des données	Les logiciels malveillants endommagent, effacent, altèrent ou suppriment des données informatiques.
Article 5 – Atteinte à l'intégrité du système	Les logiciels malveillants peuvent porter atteinte au fonctionnement d'un système informatique.
Article 6 – Abus de dispositifs	Les logiciels malveillants sont des dispositifs relevant de la définition figurant à l'article 6 (les Parties qui émettent des réserves quant à l'article 6 doivent néanmoins toujours ériger en infraction la vente, la distribution ou la mise à disposition des dispositifs visés par ledit article). Et ce parce qu'ils sont généralement conçus ou adaptés avant tout pour commettre les infractions visées aux articles 2 à 5. Par ailleurs, l'article érige en infraction pénale la vente, l'obtention pour utilisation, l'importation, la distribution ou d'autres formes de mise à disposition de mots de passe, de codes d'accès ou de données similaires permettant de s'introduire dans des systèmes informatiques. L'action pénale à l'encontre des logiciels malveillants met souvent au jour ces éléments.
Article 7 – Falsification informatique.	Les logiciels malveillants peuvent introduire, altérer, effacer ou supprimer des données informatiques engendrant des données non authentiques dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques.
Article 8 – Fraude informatique.	Les logiciels malveillants peuvent causer la perte d'un bien appartenant à une personne et permettre à une autre personne d'obtenir un bénéfice économique en introduisant, altérant, effaçant ou supprimant des données informatiques et/ou en portant atteinte au fonctionnement d'un système informatique.
Article 11 – Tentative et complicité	Les logiciels malveillants peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans le traité ou pour se rendre complices de leur commission
Article 13 – Sanctions	Les incidences des nouvelles formes de logiciels malveillants sont multiples. Certains logiciels malveillants sont relativement anodins ; d'autres présentent un danger pour les personnes, les infrastructures critiques, ou à d'autres

	niveaux. Les incidences peuvent varier selon les pays pour des raisons techniques, culturelles ou autres. Il est possible que la sanction prévue par la législation nationale de certaines Parties à l'égard des attaques perpétrées par des logiciels malveillants soit trop clémente et ne permette pas la prise en considération des circonstances aggravantes, de la tentative ou de la complicité. D'où l'éventuelle nécessité pour ces Parties d'envisager la modification de leur législation. Par conséquent, les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées à ces attaques « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris des sanctions pécuniaires. Les Parties peuvent également prendre en considération des circonstances aggravantes, par exemple si les attaques de logiciels malveillants portent atteinte à un nombre important de systèmes, provoquent des dégâts considérables, y compris des décès ou des blessures physiques, ou endommagent des infrastructures critiques.

Déclaration du T-CY

La liste des articles, présentée ci-dessus, concernant toutes les formes de logiciels malveillants illustre les multiples infractions qui peuvent être commises au moyen de ces attaques.

Par conséquent, le T-CY s'accorde à dire que toutes les formes de logiciels malveillants, sous leurs différents aspects, sont couvertes par la Convention de Budapest.

7 Note d'orientation sur l'accès transfrontalier aux données[24]

Introduction

Lors de sa 8e session plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation destinées à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions juridiques, politiques et technologiques.[25]

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes les Parties.

La présente note est consacrée à la question de l'accès transfrontalier aux données tel que visé à l'article 32 de la Convention de Budapest.[26]

L'article 32b énonce une exception au principe de territorialité en autorisant dans des circonstances limitées l'accès transfrontalier unilatéral sans passer par l'entraide judicaire. Les Parties sont invitées à utiliser plus efficacement toutes les dispositions de la Convention de Budapest portant sur la coopération internationale, notamment l'entraide judiciaire.

Dans l'ensemble, les pratiques, les procédures ainsi que les conditions et les garanties qui les accompagnent varient considérablement entre les différentes Parties. Il existe toujours des préoccupations, auxquelles il faut répondre, concernant les droits procéduraux des suspects, la protection de la vie privée et des données à caractère personnel, la base légale de l'accès aux données stockées à l'étranger ou au moyen de l'informatique en nuage, et le principe de la souveraineté nationale.

Cette note d'orientation vise à aider les Parties à appliquer la Convention de Budapest, à corriger les malentendus concernant l'accès transfrontalier en vertu de cette convention et à rassurer les tiers.

Elle aidera ainsi les Parties à exploiter pleinement les possibilités offertes par la convention en matière d'accès transfrontalier aux données.

Article 32 de la Convention de Budapest

Texte de l'article :

> 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; ou

[24] Adoptée lors de la 12ème réunion plénière du T-CY (2-3 décembre 2014)

[25] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[26] La préparation de cette note d'orientation fait suite aux conclusions du rapport intitulé « Compétence et accès transfrontalier » (T-CY(2012)3) adopté par le T-CY en décembre 2012. http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)3F_transborder_repV31public_7Dec12.pdf

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 États 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. À 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 de la Convention de Budapest par le T-CY

Concernant l'article 32a (accès transfrontalier à des données informatiques accessibles au public 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.

On considère généralement que les membres des services répressifs peuvent consulter toutes les données accessibles publiquement, et qu'à cette fin ils peuvent s'inscrire ou s'abonner aux services ouverts au public.[27]

Si une partie d'un site web, d'un service ou d'un système du même type est fermée au public alors que le reste est accessible, cette partie n'est pas considérée accessible au sens de l'article 32a.

Concernant l'article 32b, on peut envisager les situations caractéristiques suivantes :

[27] La législation nationale peut toutefois limiter l'accès à des données publiquement disponibles ou leur utilisation par les services répressifs.

- 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. Cette personne peut récupérer les données et, pourvu qu'elle y soit juridiquement habilitée, elle peut les communiquer de son propre gré aux forces de l'ordre ou leur permettre d'y accéder, tel que prévu à l'article.[28]

- Un individu suspecté de trafic de drogues est arrêté dans les règles alors que son courrier électronique est ouvert sur sa tablette, son smartphone ou un autre appareil, révélant éventuellement des preuves de délit. Si le suspect autorise de son propre gré la police à accéder à son compte et si celle-ci est certaine que les données sont localisées dans un autre Etat partie, elle peut y avoir accès en vertu de l'article 32b.

Les autres situations ne sont ni autorisées ni exclues.[29]

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

Considérations et garanties générales

L'article 32b est une mesure à appliquer dans des enquêtes et procédures pénales spécifiques dans le cadre de l'article 14.[30]
Comme il a été souligné plus haut, les Parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de primauté du droit, conformément à l'article 15 de la Convention de Budapest.[31]

---

[28] Paragraphe 294 du rapport explicatif

[29] Paragraphe 293 du rapport explicatif. Voir aussi l'article 39.3 de la Convention de Budapest.

[30] Article 14 – Champ d'application des mesures procédurales
1Chaque 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.
2Sauf 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.
3a 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.

[31] Article 15 – Conditions et sauvegardes

Les droits des individus et les intérêts des tiers doivent être pris en compte dans l'application de cette mesure.

Par conséquent, la Partie qui perquisitionne un autre Etat partie peut envisager d'informer les autorités compétentes de celui-ci.

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 ».[32]

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

L'article 32b mentionne les « données informatiques stockées situées dans un autre Etat [partie] », ce qui signifie qu'il peut être utilisé lorsqu'on sait où les données se trouvent.

L'article 32b ne prévoit pas certaines autres situations, par exemple lorsque les données ne sont pas stockées sur le territoire d'une autre Partie ou lorsqu'on n'a pas la certitude de leur lieu de stockage. Une Partie ne peut invoquer l'article 32b pour obtenir la divulgation de données stockées sur son propre territoire.

Selon l'article 32b, d'autres situations « ne sont ni autorisées ni exclues. » Ainsi, lorsqu'on ignore si les données sont stockées dans un autre Etat partie ou lorsqu'on n'en a pas la certitude, les Parties peuvent être amenées à évaluer elles-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 des considérations liées aux relations internationales.

Concernant la notion d'« accès sans autorisation de l'autre Partie »

L'article 32b n'impose pas l'utilisation de l'entraide judiciaire, et la Convention de Budapest n'exige pas que l'autre Partie soit informée. Pour autant, la convention n'exclut pas une telle notification. Les Parties peuvent informer l'autre Partie si elles le jugent utile.

---

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

[32] Paragraphe 293 du rapport explicatif de la Convention de Budapest

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 aux données ou qui consent à les divulguer ne doit avoir subi ni contrainte ni tromperie.[33]

Selon certaines réglementations nationales, il se peut que les mineurs ou les personnes souffrant de troubles mentaux ou d'autres affections ne puissent donner valablement leur consentement.

Dans la plupart des Etats parties, la coopération dans le cadre d'une enquête pénale requiert un consentement explicite. Par exemple, l'acceptation des conditions générales d'utilisation d'un service en ligne peut être insuffisante à constituer un consentement explicite, même si ces conditions indiquent que les données peuvent être transmises aux autorités judiciaires en cas d'utilisation frauduleuse.

Concernant le droit applicable

Dans tous les cas, les services répressifs doivent appliquer les mêmes normes juridiques dans l'application de l'article 32b que dans leur propre pays. Si l'accès aux données ou leur divulgation ne seraient pas autorisés sur le territoire national, il en va de même dans l'application de l'article 32b.

Les parties à la convention sont supposées se faire mutuellement confiance et respecter les principes des droits de l'homme et de la primauté du droit, conformément à l'article 15 de la Convention de Budapest.

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

S'agissant de déterminer « qui » est « légalement autorisé » à divulguer des données, cette question peut varier en fonction des circonstances ainsi que de la législation et de la réglementation en vigueur.

Il peut par exemple s'agir d'un particulier donnant accès à sa messagerie électronique ou à d'autres données qu'il a stockées à l'étranger.[34]

Il peut aussi s'agir d'une personne morale.

Il est peu probable que les prestataires de services remplissent les conditions d'un consentement valide et volontaire concernant la divulgation des données de leurs utilisateurs dans les conditions de l'article 32. En général, les prestataires de services ne sont que les dépositaires de ces données. Ils n'en ont pas le contrôle ni la propriété et ne sont donc pas dans la capacité de donner un consentement valide. En revanche, les forces de l'ordre pourront bien sûr se procurer les données dans un pays étranger par d'autres moyens, comme l'entraide judiciaire ou les procédures applicables aux situations d'urgence.

Demandes internes légalement formulées et article 32b

L'article 32b ne s'applique pas aux injonctions de produire ni à d'autres demandes légalement formulées au sein d'un Etat partie.

[33] Dans certains pays, le fait d'accepter que les poursuites soient abandonnées, ou que la gravité des chefs d'inculpation ou la durée d'une peine de prison soient réduites constitue un consentement légal et volontaire.

[34] Voir l'exemple donné dans le paragraphe 294 du rapport explicatif

Concernant la localisation de la personne consentant à fournir l'accès aux données ou à les divulguer

L'hypothèse habituelle est que la personne qui donne l'accès aux données est physiquement présente sur le territoire de la Partie requérante.

Cependant, de multiples situations sont possibles. On peut envisager que la personne physique ou morale se trouve sur le territoire des services répressifs de l'Etat requérant lorsqu'elle consent à divulguer les données ou à y donner effectivement accès ; ou uniquement lorsqu'elle consent à les divulguer mais pas à y donner accès ; ou encore qu'elle se trouve dans le pays où les données sont stockées lorsqu'elle accepte de les divulguer et/ou qu'elle y donne accès. La personne peut aussi se trouver physiquement dans un pays tiers lorsqu'elle accepte de coopérer ou lorsqu'elle donne effectivement accès aux données. S'il s'agit d'une personne morale, (comme une entité privée), elle peut être représentée simultanément sur le territoire des services répressifs requérants, sur le territoire où se trouvent les données, voire dans un pays tiers.

Il faut tenir compte du fait que de nombreuses Parties s'opposent à ce qu'une personne physiquement présente sur leur territoire soit directement approchée par des services répressifs étrangers désirant sa coopération ; certains pays considèrent même cette démarche comme une infraction pénale.

Déclaration du T-CY

Le T-CY déclare d'un commun accord que la présente note d'orientation reflète une analyse partagée par toutes les Parties quant à l'étendue et aux éléments de l'article 32.

8 Note d'orientation sur les spams[35]

Introduction

Lors de sa 8e réunion plénière (décembre 2012), le Comité de la Convention Cybercriminalité (T-CY) a décidé de publier des notes d'orientation visant à faciliter l'usage et la mise en œuvre effectifs de la Convention de Budapest sur la cybercriminalité, notamment à la lumière des évolutions du droit, des politiques et des technologies[36].

Les notes d'orientation reflètent une analyse de l'application de la Convention de Budapest partagée par toutes ses Parties.

La présente note est consacrée à la question des spams. La Convention de Budapest « utilise une terminologie technologiquement neutre de façon que les infractions relevant du droit pénal matériel puissent s'appliquer aux technologies concernées tant actuelles que futures »[37], et ce pour que des formes inédites de logiciels malveillants ou de délits restent malgré tout couvertes par la Convention.

Cette note d'orientation montre comment différents articles de la Convention s'appliquent aux spams.

Dispositions pertinentes de la Convention de Budapest sur la cybercriminalité (STE n°185)

Le spam désigne en général l'envoi en masse de courriels non sollicités. Un message est envoyé à un nombre considérable d'adresses électroniques et l'identité personnelle du destinataire n'entre pas en ligne de compte car le message est adressé de la même manière à beaucoup d'autres destinataires, sans distinction.

Des questions distinctes se posent concernant les points suivants :

- le contenu du spam ;
- l'acte d'envoyer un spam, et ;
- le dispositif utilisé pour transmettre un spam.

Le contenu du spam peut être illégal ou non. Lorsqu'il l'est (comme la proposition de médicaments contrefaits ou des offres financières frauduleuses), l'infraction peut relever de la législation nationale pertinente en la matière. L'acte de transmettre un spam (y compris la transmission à grande diffusion de contenus non-répréhensibles) peut constituer une infraction civile ou pénale dans certaines juridictions.

La Convention ne couvre pas les spam dont le contenu n'est pas illégal et ne pas porter une atteinte à l'intégrité du système, mais qui peut-être être nuisibles aux utilisateurs finaus.

Les outils utilisés pour transmettre des spams peuvent être illégaux en vertu de la Convention de Budapest, et les spams peuvent être associés à d'autres infractions qui ne sont pas mentionnées dans le tableau ci-dessous (voir, par exemple, les articles 7 et 8).

Comme pour d'autres notes d'orientation, chaque disposition contient un critère d'intention (« sans autorisation », « avec une intention frauduleuse », etc.). Dans certains cas de spams, cette intention peut être difficile à prouver.

[35] Adoptée lors de la 12ème réunion plénière du T-CY (2-3 décembre 2014)

[36] Voir le mandat du T-CY (article 46 de la Convention de Budapest).

[37] Paragraphe 36 du rapport explicatif.

Interprétation par le T-CY des dispositions relatives aux spams

Articles pertinents	Exemples
Article 2 – Accès illegal	Les spams peuvent contenir des logiciels malveillants qui peuvent accéder ou permettre d'accéder à un système informatique.
Article 3 – Interception illégale	Les spams peuvent contenir des logiciels malveillants qui peuvent intercepter illégalement ou permettre l'interception illégale de transmissions de données informatiques.
Article 4 – Atteinte à l'intégrité des données	Les spams peuvent contenir des logiciels malveillants qui peuvent endommager, effacer, détériorer, altérer ou supprimer des données informatiques.
Article 5 – Atteinte à l'intégrité du système	La transmission de spams peut entraver gravement le fonctionnement des systèmes informatiques. Les spams peuvent contenir des logiciels malveillants qui peuvent entraver gravement le fonctionnement des systèmes informatiques.
Article 6 – Abus de dispositifs	Les dispositifs relevant de la définition figurant à l'article 6 peuvent servir à transmettre des spams. Les spams peuvent contenir des dispositifs relevant de la définition de l'article 6.
Article 8 – Fraude informatique	Les spams peuvent servir comme un dispositif d'entrée, de modification, d'effacement ou de suppression de données informatiques ou d'interférence avec le fonctionnement d'un système informatique pour se procurer des avantages économiques illégaux.
Article 10 – Atteinte à la propriété intellectuelle et aux droits connexes	Les spams peuvent servir à faire de la publicité pour la vente de biens contrefaits, notamment des logiciels ou d'autres éléments protégés par les lois relatives à la propriété intellectuelle.
Article 11 – Tentative et complicité	Les spams et la transmission de spams peuvent être utilisés pour tenter de commettre plusieurs des infractions spécifiées dans la Convention ou pour se rendre complice de leur commission (telles que la falsification informatique, article 7 ; la fraude informatique, article 8).
Article 13 – Sanctions	Les spams peuvent être utilisés à de multiples fins criminelles, dont certaines ont une incidence grave sur les personnes, ou les institutions publiques ou privées. Si une Partie n'érige pas en infraction pénale le spam en tant que tel, elle devrait ériger en infraction pénale tout agissement lié aux spams tel que les infractions susmentionnées, et permettre la prise en considération de circonstances aggravantes, de la tentative ou de la complicité. Les Parties devraient faire en sorte, conformément à l'article 13, que les infractions pénales liées aux spams « soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté ». Pour les personnes morales, il peut s'agir de sanctions pénales ou non pénales, y compris de sanctions pécuniaires.

Déclaration du T-CY

La liste des articles présentée ci-dessus illustre les multiples infractions qui peuvent être commises au moyen des spams et les infractions liées aux spams.

Par conséquent, le T-CY s'accorde à dire que les spams, sous leurs différents aspects, sont couverts par la Convention de Budapest.