www.coe.int/TCY

Strasbourg, 10 May 2015 T-CY (2015)03

Cybercrime Convention Committee (T-CY)

Assessing implementation of the Budapest Convention on Cybercrime

Questionnaire on Sanctions and Measures (Article 13)

[DRAFT for consideration by the 13th Plenary of the T-CY]

Background:

The purpose of the questionnaire is to allow the T-CY Plenary to assess the implementation of Article 13 of the Budapest Convention on Cybercrime by State Parties in line with Article 2 of the T-CY Rules of Procedure.

The Cybercrime Convention Committee (T-CY), in its 11th Plenary Session (17-18 June 2014) decided to dedicate the 3rd round of assessments to Article 13 (sanctions and measures). The 13th Plenary (2-3 December 2014 invited the Bureau to prepare a draft questionnaire for consideration by the 13th Plenary (June 2015).

Implementation:

T-CY representatives are invited to prepare/compile consolidated replies to this questionnaire from their respective country.

Replies should be submitted no later than **15 October 2015** in electronic form and in English or French to:

Alexander Seger, Executive Secretary of the Cybercrime Convention Committee, Council of Europe
Email: alexander.seger@coe.int

The Bureau will then provide an initial summary to T-CY 14 (December 2015), and a full draft report by March 2016 for consideration by T-CY 15 (June 2016).

1 Criminal sanctions

1.1 General provisions

Q 1.1.1 Please provide the text of your general provisions regarding criminal liability and sanctions

Intent, negligence/recklessness	
Aggravating/mitigating circumstances	
Requirements for suspension	
Minimum/maximum penalty	
Alternative or cumulative sanctions	
Multiple crimes, recidivism	
Incitement, aiding, abetting and attempt	
Other general provisions	

1.2 Criminal sanctions for natural persons

Q 1.2.1 Sanctions for illegal access to a computer system

Budapest Convention **Art. 2 Illegal access to a computer system**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum, maximum penalty	
Attempt	
Additional comments	

Q 1.2.2 Sanctions for illegal interception

Budapest Convention **Art. 3 Illegal interception**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.3 Sanctions for data interference

Budapest Convention **Art. 4 Data interference**	1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.4 Sanctions for system interference

Budapest Convention **Art. 5 System interference**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.5 Sanctions for misuse of devices

Budapest Convention **Art. 6 Misuse of Devices**	See appendix
Corresponding domestic provision:	
Intent, negligence/recklessness	

Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.6 Sanctions for computer-related forgery

Budapest Convention Art. 7 Computer-related forgery	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.7 Sanctions for computer-related fraud

Budapest Convention Art. 8 Computer-related fraud	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.8 Sanctions for computer-related fraud

Budapest Convention Art. 9 Child pornography	See appendix

Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.9 Sanctions for Offences related to infringements of copyright and related rights

Budapest Convention **Art. 10 Offences related to infringements of copyright and related rights**	Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.
Corresponding domestic provision:	
Intent, negligence/recklessness	
Aggravating circumstances	
Minimum/maximum penalty	
Attempt	
Additional comments	

Q 1.2.10 Are there any Domestic Guidelines for Judges while imposing certain criminal sanction, specifically for the crimes enshrined in Articles 2-11 of the Convention on Cybercrime?

Q 1.2.11 Does national legislation allow for using a combination of several criminal sanctions (e.g deprivation of liberty, fine,) against natural persons for crimes described in Articles 2-11 of the Convention on Cybercrime and under what circumstances?

1.3 Liability of legal persons

Q 1.3.1 Are legal persons liable for the crimes corresponding to those enshrined in Articles 2-11 of the Convention on Cybercrime?

Q 1.3.2 What are the corresponding applicable sanctions?

2 Other measures

2.1 Confiscation

Q 2.1.1 Does national legislation allow confiscation of the means that have been used to commit a criminal offence?

Q 2.1.2 What are the legal requirements?

Q 2.1.3 Does national legislation allow confiscation of the crime proceed, including from third persons?

Q 2.1.4 What are the legal requirements?

3 Statistics on sanctions and measures

Q 3.1.1 Please provide, if available data/statistics on sanction and measures

4 Case law

4.1 Typical examples of sanctions for natural persons

Q 4.1.1 Please provide examples of sanctions for natural persons? What have been average sanctions for natural persons? Suspended sentences, probation?

4.2 Typical examples of sanctions for legal persons

Q 4.2.1 Please provide examples of sanctions for legal persons? What have been average sanctions for legal persons?

4.3 Practice concerning confiscation

Q 4.3.1 What is the case law regarding confiscation?

Appendix: Extracts of the Budapest Convention on Cybercrime

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Rapport explicatif

Sanctions et mesures (article 13)

128. Cet article est étroitement lié aux articles 2 à 11, qui définissent différentes infractions informatiques ou en relation avec l'ordinateur qui doivent être rendues passibles de sanctions pénales. Conformément aux obligations imposées par ces articles, cette disposition oblige les Parties contractantes à tirer les conséquences de la gravité de ces infractions en prévoyant des sanctions pénales qui soient 'effectives, proportionnées et dissuasives' et, dans le cas des personnes physiques, incluent la possibilité d'imposer des peines d'emprisonnement.

129. Les personnes morales dont la responsabilité doit être établie en vertu de l'article 12 doivent également être exposées à des sanctions 'effectives, proportionnées et dissuasives', pouvant être pénales, administratives ou civiles. Les Parties contractantes sont tenues, en application du paragraphe 2, de prévoir la possibilité d'imposer des sanctions pécuniaires aux personnes morales.

130. L'article laisse ouverte la possibilité d'imposer d'autres sanctions ou mesures adaptées à la gravité des infractions commises – par exemple des ordonnances d'interdiction ou de confiscation. Il laisse à l'appréciation des Parties la question de la création d'un système d'infractions et de sanctions pénales qui soit compatible avec leur ordre juridique interne.

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux Article 5 – System interference

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;

ii 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,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de 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, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui:

a par toute introduction, altération, effacement ou suppression de données informatiques;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme «pornographie enfantine» comprend toute matière pornographique représentant de manière visuelle:

a un mineur se livrant à un comportement sexuellement explicite;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.