

ASSOCIATION INTERNATIONALE DE DROIT PENAL  
INTERNATIONAL ASSOCIATION OF PENAL LAW  
ASOCIACIÓN INTERNACIONAL DE DERECHO PENAL



Lettre d'information

Newsletter

Carta informativa

1/2012

## SOMMAIRE

Message du Président	3
La Vie de l'Association	4
Les Activités Scientifiques de l'Association	5
La Revue et les Autres Publications de l'Association	7

## SUMMARY

Message of the President	8
The Life of The Association	9
The Scientific Activities of the Association	10
The International Review of Pénal Law and Other Publications	12
Section 1: Questionnaire and annexes	13
Section 2: Questionnaire and annexes	20
Section 3: Questionnaire and annexes	33
Section 4: Questionnaire and annexes	42

## SUMARIO

Mensaje del Presidente	51
La Vida de la Asociación	52
Las Actividades Científicas de la Asociación	53
La Revue y las Demás Publicaciones de la Asociación	55
Sección 1: Cuestionario y anexo	56
Sección 2: Cuestionario y anexo	61
Sección 3: Cuestionario y anexo	68
Sección 4: Cuestionario y anexo	72

## MESSAGE DU PRÉSIDENT

*José Luis de la Cuesta*  
*Président*

Chers collègues et amis, membres de l'Association Internationale de Droit Pénal (AIDP-IAPL),

Une fois de plus cette année, j'ai le plaisir d'accompagner de mes vœux la Newsletter qui a été soigneusement préparée sous la direction de la Secrétaire Générale, Katalin Ligeti, en vue d'informer nos membres de la vie de l'Association et, en particulier, des résolutions adoptées par le comité exécutif lors de la réunion tenue à l'ISISC (Syracuse, Italie), les 3 et 4 décembre.

Le travail des membres dirigeants de l'Association ces derniers mois a été intense et a porté premièrement sur la préparation du colloque préparatoire, lequel, selon notre méthodologie, doit servir à préparer les propositions de résolutions qui seront débattues à chaque session de notre XIXème congrès international de droit pénal, prévu à Rio de Janeiro (Brésil) en 2014. Dans ce but, grâce à l'hospitalité de notre collègue Ulrich Sieber, Directeur du Max-Planck Institute à Freiburg, les 20 et 21 novembre, le Vice-président John Vervaele et la Secrétaire Générale Ligeti ont pu avoir une réunion très productive avec les rapporteurs généraux des quatre sections. Le résultat de cette réunion est la finalisation des quatre questionnaires, qui ont déjà été approuvés par le comité exécutif et sont contenus dans cette Newsletter (et seront publiés sur la page internet de l'Association), afin de permettre une distribution générale et en vue de permettre la préparation des rapports nationaux présentés à chaque colloque préparatoire par la personne désignée par chaque groupe national.

Notre Vice Président Jean-François Thony est également en train de travailler de manière intense avec les autorités monégasques afin de s'assurer que la conférence mondiale, préparée par notre Vice Président Helmut Epp, pourra se tenir à Monaco, éventuellement à l'automne 2012.

S'agissant des jeunes pénalistes, après avoir tenu leur deuxième Symposium international (La Rochelle, France, 29 septembre – 1er octobre 2011), ils sont actuellement en train de préparer la publication des travaux de cette importante activité dont le résultat fut un grand succès.

De plus amples informations sur ces événements et d'autres événements plus importants de la vie de l'Association sont contenus dans la présente Newsletter, que l'on fera circuler entre les membres en janvier. En conséquence, je voudrais utiliser cette opportunité pour souhaiter à l'ensemble des membres mes meilleurs vœux pour la nouvelle année 2012.

José Luis de la Cuesta

## LA VIE DE L'ASSOCIATION

*Katalin Ligeti*  
*Secrétaire Général*

Chers collègues et amis,

Le comité exécutif a consacré son travail au cours du second semestre 2011 à la mise en place du nouveau programme scientifique de l'AIDP adopté en juin 2010. Quant au nouveau programme scientifique vous pouvez retrouver tous les détails dans la partie écrite par le Vice-président John Vervaele. Permettez-moi alors de vous informer sur les questions administratives suivantes:

### Nouveau siège de l'Association

Grâce aux efforts du Vice-président Jean-François Thony, l'Association dispose déjà des clefs et le contrat de location a été signé. Le bureau est situé rue Ferrus (à côté de la place d'Italie) et inclut une salle de réunion ainsi qu'une place où les archives de l'Association peuvent être entreposées. Le bureau dispose également de deux places de parking. L'Association avait rassemblé une collection importante de livres qui est pour le moment stockée à Pau, mais devrait être transférée au siège de l'Association.

### Nouvelle brochure de l'AIDP

Le nouveau logo ainsi que le document de promotion de l'AIDP ont été finalisés avec l'aide de fonds fournis par le gouvernement espagnol. Les brochures de l'AIDP sont épuisées et il s'organisera pour éditer 3000 copies supplémentaires (anglais, français et espagnol). Carlos Japiassù préparera la version portugaise de la brochure. Les groupes nationaux qui souhaitent recevoir les brochures peuvent s'adresser au Secrétariat de l'Association.

### Divers

Notre Président, Jose Luis de la Cuesta, s'est vu décerné le titre de Doctor Honoris Causa par l'Université Alexandru Ioan Cuza, en hommage à son précieux travail dans le domaine du droit pénal et des sciences criminelles. La proposition a été faite par la faculté de droit de l'Université, la plus ancienne de Roumanie où figure dans la galerie de ses plus grands professeurs Vespasian V. Pella, Président de l'AIDP entre 1946 et 1952. La cérémonie de remise du titre s'est déroulée le 28 octobre 2011 dans la Aula Magna de l'Université.

Permettez-moi de profiter de cette occasion pour vous informer que la prochaine réunion du Conseil de Direction avec les représentants des Groupes Nationaux ainsi que la réunion du Comité exécutif et du Comité scientifique avec le Comité de la Revue auront lieu les 1er et 2 Juin 2012 à Paris.

## LES ACTIVITES SCIENTIFIQUES DE L'ASSOCIATION

*John Vervaele*  
*Vice-président*

La préparation du 19<sup>ème</sup> congrès international de droit pénal et les quatre colloques préparatoires.

Nous continuons la préparation du 19<sup>ème</sup> congrès international de la société de l'information et de la justice pénale. Le 19<sup>ème</sup> congrès international de droit pénal se tiendra en septembre 2014 et sera organisé par le groupe national brésilien dans le cadre de la coopération entre l'AIDP et l'Institut Brésilien de Sciences Criminelles (IBCCrim, São Paulo). Le secrétaire général adjoint Carlos Japiassú devrait présenter la première épreuve du programme en juin à Paris.

Le colloque préparatoire sera organisé par les groupes nationaux turcs et italiens, ainsi que le groupe national russe en collaboration avec le congrès russe de droit pénal et le groupe national finlandais. Le calendrier pour le colloque préparatoire sera le suivant :

Section 1 : Vérone (Italie) – 29 novembre -1 décembre 2012  
Section 2 : Moscou (Russie) – 24-27 avril 2013  
Section 3 : Antalya (Turquie) – Septembre 2013  
Section 4 : Helsinki (Finlande) – la semaine du 10-15 juin 2013

Les quatre experts sont:

Prof. dr. T. Weigend , Section 1, partie générale  
Prof. dr. E. Viano, Section 2, partie spéciale  
Prof. dr. H. Nijboer, Section 3, procédure pénale  
Prof. dr. A. Klip, Section 4, droit pénal international

Après la réunion des rapporteurs qui s'est tenue en juin à Paris, les rapporteurs ont élaboré un projet de texte pour leur session ainsi qu'un projet de questionnaire. Ces projets ont été discutés de manière approfondie au séminaire spécial d'expertise du Max Planck Institute à Freiburg, grâce à la générosité du Prof. U. Sieber. Prof. U. Sieber, Prof. J. Vervaele, Prof. Katalin Ligeti, dr. Els de Busser et N. von zur Muehlen de même que les quatre rapporteurs généraux étaient présents à ce séminaire. .

Le résultat du séminaire d'expertise a été intégré dans le projet de texte et dans les projets de questionnaires par les rapporteurs généraux et soumis au comité exécutif à la réunion de Syracuse en décembre.

La réunion de Syracuse a approuvé le résultat final des préparations, inclut dans cette Newsletter. Cette Newsletter, ensemble avec le texte et le questionnaire pour les quatre sessions, sera envoyée à l'ensemble des groupes nationaux avec la demande de participer activement à l'élaboration des rapports nationaux. Je voudrais utiliser cette opportunité pour remercier Prof. Chris Blakesley de sa correction de la version anglaise des questionnaires ainsi que le Prof. Isidoro Blanco pour la traduction espagnole des textes.

Suivant la méthodologie des précédents congrès, des experts sélectionnés devraient travailler sur les rapports régionaux et spéciaux. Le Comité exécutif recommande les thèmes suivants pour les rapports spéciaux et régionaux:

1. Rapports spéciaux:
  - Responsabilité pour les violations des droits de l'Homme commises par l'ICT
  - Les droits de la défense et l'usage de l'informatique dans la procédure pénale
  - Souveraineté dans le cyber espace (thème qui sera préparé par un juriste de droit international public)
  - Raisons de la protection des données
2. Rapports globaux et régionaux
  - Pour la section 1: Réseaux sociaux et infractions commises par informatique (qui sera préparé par Stanislaw Tosza)
  - Pour la section 2: La convention sur le cyber crime et les développements récents
  - Pour la section 3: Les initiatives européennes concernant l'utilisation de l'informatique dans la procédure pénale et la protection des données (qui sera préparé par Joachim Vogel et Els de Busser)

Les participants décident de proposer au Comité des Jeunes Pénalistes de désigner des rapporteurs pour les rapports spéciaux. Le Comité des Jeunes Pénalistes pourrait suggérer que d'autres sujets fassent l'objet de rapports spéciaux. Les rapporteurs généraux pourraient également suggérer des candidats pour la rédaction des rapports spéciaux.

#### Symposium des jeunes pénalistes sur la justice transnationale

Le 2nd Symposium des jeunes pénalistes sur la justice transnationale s'est tenu à la Rochelle (France) entre le 29 septembre et le 1er octobre 2011. Le Symposium a été co-organisé par le comité des jeunes pénalistes de l'AIDP, le Centre d'Études Juridiques et Politiques (CEJEP) et l'Université de la Rochelle (France). La conférence a été sponsorisée par la région Poitou-Charentes, le département de la Charente-Maritime et la ville de la Rochelle. Le symposium a autorisé les jeunes pénalistes à présenter leurs recherches dans le domaine de la justice transnationale. 21 papiers ont été sélectionnés par le comité scientifique et ont été présentés durant les 5 sessions de travail présidés par des professeurs de droit pénal venant d'Espagne, de France et d'Italie. Environ 50 jeunes pénalistes de 23 pays (couvrant 5 continents) participèrent à l'événement. La session d'ouverture a été honorée de la présence du Président De la Cuesta, qui prononça un discours sur l'histoire et les activités de l'AIDP. Le juge Wolfgang Schomburg prononça le discours d'ouverture. La session finale s'acheva avec les remarques conclusives de Carla del Ponte, ancien procureur du ICTY et ICTR.

Actuellement les travaux du symposium sont édités par le Comité scientifique et seront publiés en 2012.

#### Préparation de la conférence mondiale en 2011

Le Vice-président Epp est actuellement en train de négocier l'organisation de la conférence mondiale sur le crime environnemental à Monaco. La conférence pourrait se situer en automne 2012.

S'il était impossible d'organiser la conférence mondiale à Monaco, il pourrait être possible la tenir à Manaus (Brésil).

Je voudrais exprimer mes profonds regrets au sujet du décès de notre collègue et ami Günter Heine, qui avait été nommé rapporteur général de la conférence mondiale. Une fois le lieu de la conférence mondiale décidé, l'AIDP devra désigner le plus vite possible le nouveau rapporteur général.

#### Conférences régionales

Le groupe national turc de l'AIDP et le groupe national allemand ont organisé ensemble une conférence régionale sous le titre de « Cyber crime : un dialogue juridique germano-turc ». La conférence s'est tenue à Istanbul du 13 au 15 octobre 2011. Le Vice-président Vervaele et la Secrétaire-General Ligeti ont participé à la conférence.

Le groupe national roumain planifie l'organisation d'une conférence régionale à Bucarest en mai 2012.

Le Président Honoraire Cherif Bassiouni a proposé au cours du meeting du Conseil de Gouvernance de l'ISISC de mettre en place une importante conférence de l'AIDP en 2012 afin de célébrer le 40<sup>ème</sup> anniversaire de l'ISISC. Plus d'information au sujet de l'organisation de cet événement devrait être présentées à la réunion de Juin à Paris.

## LA REVUE ET LES AUTRES PUBLICATIONS DE L'ASSOCIATION

*Jacques Buisson*  
*Directeur de la Revue*

### Plan de publication de la Revue

- RIDP 2011 3-4 : Divers (Rédacteur en Chef : Isidoro Blanco; Senior Carlos Japiassú)
- RIDP 2012 1-2 : La justice négociée (Senior : Thomas Weigend)
- IRLP 2012 3-4: Droit de représentation propre (Senior: Juan-Luis Colomer),
- IRLP 2013 1-2: Formes de perpétration des infractions en groupe (Senior: Thomas Weigend)

### Nouvelles Études Pénales (NEP)

L'Association planifie de publier dans les trois langages officiels de l'AIDP les résolutions de tous les Congrès incluant les résolutions du dernier congrès. De plus, la prochaine parution de la NEP devrait contenir les documents légaux mis à jour (statuts, règlements) de l'Association.

### Divers

L'Association assurera la publication des documents du Symposium des Jeunes Pénalistes à La Rochelle.

## MESSAGE OF THE PRESIDENT

*José Luis de la Cuesta*  
*President*

Dear colleagues and friends, members of the International Association of Penal Law (AIDP-IAPL),

Again, this year, I have the pleasure to accompany with my greetings the newsletter carefully prepared under the direction of the Secretary General, Katalin Ligeti, in order to keep our members informed of the life of the Association and, in particular, about the resolutions adopted by the Executive Committee at the meeting held at the ISISC (Siracusa, Italy), on 3 and 4 December.

The work of the governing bodies of the Association these last months has been intense and has focused primarily on the preparation of the preparatory colloquia, which, according to our methodology, shall serve as the preparation for proposals for resolutions to be debated at every session of our XIX International Congress of Penal Law, which will be held in Rio de Janeiro (Brazil) in 2014. For this purpose, thanks to the hospitality of our colleague Ulrich Sieber, Director of the Max-Planck Institute in Freiburg, on 20 and 21 November Vice-President John Vervaele and Secretary General Ligeti were able to hold a very productive meeting with the general rapporteurs of the four sections. The result of that meeting is the completion of the four questionnaires, which have already been approved by the Executive Committee and are contained in this Newsletter (and will be posted on the web-page of the Association), for the purposes of general distribution and in order to allow the preparation of national reports presented at each preparatory colloquium by the person designated by each national group.

Our Vice President Jean-François Thony is also working intensively with the Monegasque authorities to ensure that the World Conference, prepared by our Vice President Helmut Epp, can take place in Monaco, possibly in the autumn of 2012.

As to the Young Penalists, after having held their Second International Symposium (La Rochelle, France, 29 September - 1 October 2011), they are currently preparing the publication of the proceedings of this important activity that resulted as great success.

More detailed information about these and other important events in the life of the Association is contained in the present Newsletter, which will be circulated among the members in January. Therefore I would like to use this opportunity to wish to all the members of the Association all the best for the New Year 2012.

José Luis de la Cuesta

## THE LIFE OF THE ASSOCIATION

*Katalin Ligeti*  
*Secretary General*

Dear colleagues and friends,

The Executive Committee dedicated its work in the second half of 2011 to continue implementing the new scientific programme of the AIDP adopted in June 2010. With respect to the new scientific programme you will find all details in the subsection written by Vice President John Vervaele. Let me therefore refer you to the following selected administrative issues:

### **New seat of the Association**

Thanks to the efforts of Vice-President Thony, the Association already has the keys of the new seat of the AIDP in Paris and the formal lease agreement has been signed. The office is situated at Rue Ferrus (near Place d'Italie) and includes a meeting room and a place where the archives of the Association can be stored. Two parking places belong to the office as well. The Association gathered an important collection of books that are for the moment stored in Pau and should be now moved to the seat of the Association.

### **New flyer of the AIDP**

The new logo and advertising materials for the AIDP have been finalised with the help of the subsidy granted by the Spanish government. The flyers of the AIDP had run out and another 3000 copies are being printed (English, French, Spanish). Carlos Japiassú will prepare the Portuguese version of the flyer. The National Groups who are interested in receiving the flyers can address the Secretariat of the Association.

### **Miscellaneous**

Our President, Jose Luis de la Cuesta, has been awarded the title of Doctor Honoris Causa by the Alexandru Ioan Cuza University, in appreciation of his valuable work in the field of Criminal Law and Criminal Sciences. The proposal was made by the Faculty of Law of the University, the oldest in Romania and which includes in the gallery of its greatest professors, Vespasian V. Pella, President of the AIDP between 1946 and 1952. The Ceremony conferring the title took place on October 28 in the Aula Magna of the University.

Let me use this opportunity to inform you that the next meeting of the Board of Directors together with the representatives of the National Groups as well as the meeting of the Executive Committee and the Scientific Committee together with the Committee of the Review will take place on 1 and 2 June 2012 in Paris.

## THE SCIENTIFIC ACTIVITIES OF THE ASSOCIATION

*John Vervaele*  
*Vice President*

### Preparation of the 19th International Congress of Penal Law

We are continuing to prepare the 19th International Congress on Information Society and Criminal Justice.

The 19th International Congress will be held in Rio de Janeiro in September 2014 and will be organized by the Brazilian National Group in cooperation with the AIDP-partner, the Brazilian Institute of Criminal Sciences (IBBCRIM). Deputy Secretary General Carlos Japiassú shall present the first draft of the programme at the meeting of the the Board of Directors in June 2012 in Paris.

The preparatory colloquia will be organized by the Italian and Turkish national groups as well as the Russian National Group in collaboration with the Russian Congress of Criminal Law and the Finnish National Group. The schedule for the preparatory colloquia will be as follows:

- Section 1: Verona (Italy) – 29 November - 1 December 2012
- Section 2: Moscow (Russia) – 24-27 April 2013
- Section 3: Antalya (Turkey) – September 2013
- Section 4: Helsinki (Finland) – the week of 10-15 June 2013.

The four general rapporteurs are:

- Prof. dr. T. Weigend , session 1, general part
- Prof. dr. E. Viano, session 2, special part
- Prof. dr. H. Nijboer, session 3, criminal procedure
- Prof. dr. A. Klip, session 4, international criminal law

After the appointment of the general rapporteurs in the June meeting in Paris, the rapporteurs have elaborated a draft guiding text for their session and a draft questionnaire. These drafts have been discussed in depth at a special 2 days expert seminar at the Max Planck Institute in Freiburg, thanks to the hospitality of Prof. U. Sieber. Prof. U. Sieber, Prof. J. Vervaele, Prof. Katalin Ligeti, dr. Els de Busser and N. von zur Muehlen and the four general rapporteurs were present at the expert seminar.

The outcome of the expert seminar has been integrated in the draft guiding texts and draft questionnaires by the general rapporteurs and submitted to the Executive Committee at the Siracusa meeting in December.

The Siracusa meeting has approved the final outcome of the preparations, included in this newsletter. This newsletter, together with the guiding text and questionnaire for the fours sessions, will be sent to all the national groups with the request to participate actively in the elaboration of national reports. I would like to use this opportunity to thank to Prof. Chris Blakesley for reviewing the English version of the questionnaires as well as to Prof. Isidoro Blanco for the Spanish translation of the texts.

Following the methodology of the previous congresses, selected experts shall work on special and regional reports. The Executive Committee recommended the following themes for special and regional reports:

1. Special reports:
  - Accountability for human rights violations committed by information technology
  - Defence rights and the use of information technology in criminal procedure
  - Sovereignty in cyber space (to be prepared by an international public lawyer)
  - Reasons of data protection
2. Global and regional reports
  - For Section 1: Social networks and violations committed by information technology (to be prepared by Stanislaw Tosza)
  - For section 2: The Convention on Cybercrime and recent developments
  - For section 3: European initiatives concerning the use of information technology in criminal procedure and data protection (to be prepared by Joachim Vogel and Els de Busser)

The participants decided to propose to the Young Penalists Committee to designate rapporteurs for the special reports. The Young Penalists Committee may suggest further topics for special reports. The general rapporteurs may also suggest candidates for drafting the special reports.

#### Young Penalists Symposium on Transitional Justice

The 2nd Young Penalists Symposium on Transitional justice took place in La Rochelle (France) between 29 September and 1st October 2011. The Symposium was co-organised by the Young Penalists' committee of the AIDP and Centre d'Études Juridiques et Politiques (CEJEP), University of La Rochelle (France). The conference was sponsored by the Poitou-Charentes region, the Charente-Maritime department, and the Commune of the City of La Rochelle. The symposium allowed young penalists to present their research in the domain of Transitional justice. 21 papers were selected by the scientific committee and were presented during the 5 working sessions chaired by professors of criminal law coming from Spain, France and Italy. Around 50 Young Penalists from 23 countries (covering 5 continents) participated in the event. The opening session was honoured by the presence of President De la Cuesta, who gave a speech on the history and the activities of the AIDP. Judge Wolfgang Schomburg gave the keynote speech. The final session ended with concluding remarks of Carla del Ponte, ex-Prosecutor of the ICTY and ICTR.

Currently, the works of the symposium are being edited by the scientific committee to be published in 2012.

#### The preparation of the AIDP World Conference in 2011

Vice-President Epp is currently negotiating the organisation of the World Conference on environmental crime in Monaco. The conference could take place in autumn 2012.

If it would be impossible to host the World Conference in Monaco, it might be possible to organise it in Manaus (Brazil).

I would like to express my deepest regret due to the sudden death of our colleague and friend Günter Heine, who had been appointed general rapporteur of the World Conference. Once the new venue of the conference is decided, the AIDP shall choose designate a new general rapporteur as soon as possible.

#### Regional conferences

The Turkish National Group of the AIDP together with the German National Group organised a regional conference under the title: "Cybercrime: Ein deutsch-türkischer Rechtsdialog". The conference took place in Istanbul on 13-15. October 2011. Vice-president Vervaele and Secretary-General Ligeti did participate at the conference.

The Romanian National Group is planning to organise a regional conference in Bucharest in May 2012.

The Honorary President Cherif Bassiouni proposed in course of the meeting of the Governing Board of ISISC to hold an important conference of the AIDP in 2012 for celebrating the 40th anniversary of ISISC. More information about the organisation of this event shall be presented at the meeting in June in Paris.

## THE INTERNATIONAL REVIEW OF PENAL LAW AND OTHER PUBLICATIONS

*Jacques Buisson*  
*Director of the Review*

### Publication plan of the Review

- IRLP 2011 3-4: Miscellaneous (editor: Isidoro Blanco / senior: Carlos Japiassú),
- IRLP 2012 1-2: Negotiated justice (senior: Thomas Weigend)
- IRLP 2012 3-4: Right to self-representation (senior: Juan-Luis Colomer),
- IRLP 2013 1-2: Forms of perpetration in group offences (senior: Thomas Weigend)

### Nouvelles Études Pénales (NEP)

The Association is planning to publish in the three official languages of the AIDP the resolutions of all of the Congresses including the resolutions of the last Congress. Moreover the next issue of the NEP should contain the updated legal documents (Statutes, By-laws) of the Association.

### Miscellaneous

The Association will support the publication of materials of the Young Penalist Symposium of La Rochelle.

## Section 1: Concept paper and questionnaire

Thomas Weigend

### (A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with “cyber crime.” This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Thomas Weigend: [thomas.weigend@uni-koeln.de](mailto:thomas.weigend@uni-koeln.de)

### (B) Criminalisation

Please note that in this questionnaire only general characteristics of cyber crime offense definitions are of interest. Specific questions of individual crime definitions will be discussed in Section II of the Congress.

- (1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?
- (2) Please give typical examples of criminal laws concerning
  - (a) attacks against IT systems
  - (b) violation of IT privacy
  - (c) forgery and manipulation of digitally stored data
  - (d) distribution of computer viruses
  - (e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities
  - (f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.
- (3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined (“data”, “writings”, contents)?
- (4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?
- (5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?
- (6) Are there specific differences between the definition of cyber crimes and “traditional” crimes?

### (C) Legislative technique

- (1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?
- (2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the internet?
- (3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,
  - how are changes in the use of internet and social networks taken into account?
  - how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

### (D) Extent of criminalisation

- (1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for “hacking”, “phishing”, computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

- (2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?
- (3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea? Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?
- (4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?
- (5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

#### (E) Alternatives to Criminalisation

- (1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?
- (2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?
- (3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

#### (F) Limiting anonymity

- (1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?
- (2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?
- (3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

#### (G) Internationalisation

- (1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?
- (2) To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?
- (3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

#### (H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

## Annex 1

John A.E. Vervaele

### (1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society (Castells 1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

### (2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

#### 1. The integrity and functionality of the cyber-ICT system (CIA offences)

2. Protection of privacy
3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Annex 2

### General considerations

Thomas Weigend

#### (1) Information technology in need of protection

To an extent that was hardly foreseeable even 30 years ago, social life on a worldwide scale depends on the proper functioning of information and communication technology (ICT) and the internet. This dependence extends to both the public and the private spheres. On an individual level, interpersonal communication, but also large parts of leisure activity including information-gathering are ICT-based, and many individuals have heavily invested in the development and maintenance of their digital personality (or personalities), e.g. in personal websites and blogs or communication services such as Facebook and Twitter.

These developments have led to a situation where attacks on the integrity of ICT have become serious threats that can affect not only individual interests but also the security of states, important business interests, and the economic system as a whole. Hacking and data falsification, violations of the privacy of digitally transmitted communications, and "identity theft" on the internet are threatening the well-being not only of individuals but also of business firms and states.

#### (2) Information technology and the worldwide web as a means to commit crime

ICT also has transformed the quantitative dimension of certain assaults on legally protected interests. Whereas in earlier times persons with criminal intentions to defraud or to spread libellous information had to approach each potential recipient of information individually, it is now possible to spread information to hundreds of thousands of persons within a second by using automated e-mail services or websites. The use of computer viruses to create bot networks can further multiply the effectiveness of an assault and involve up to a million of computers belonging to persons who are unaware of the fact that their addresses are being misused. The existence of a worldwide web and the possibilities of computer technology thus enable persons with criminal intentions to cause maximal harm with minimal effort.

Other features of ICT further contribute to the attractiveness of the net for criminal assaults on individual or collective interests. The possibility of acting anonymously and of using a false identity enables criminals to remain undetected. Detection is further complicated by the extremely high speed of data transfer coupled with routine deletion of transfer data by service providers. The origins of the worldwide web as a device for the quick transfer of secret military information further contribute to the shielding of network users from detection: the worldwide web was purposely devised as a network with many overlapping and independent lines of communication, thus making the web resistant to any attempt of disturbing its functioning through external intervention. The web structure also makes it highly difficult to trace individual items of information back to one source or to effectively block access to an information.

#### (3) The Role of the Criminal Law

##### (a) Protecting ICT against Crime

The special sensitivity of ICT to criminal attacks, and the great harm that can be caused by such attacks, make it necessary to employ the criminal law in preventing and sanctioning acts that interfere with the integrity of communications based on ICT. Many legal systems have enacted criminal provisions dealing with such phenomena as data theft, data falsification, and invading protected data bases. Due to the inherently transnational character of the worldwide web, international organisations have attempted to harmonize national legislation in this area (see, e.g., the Cybercrime Convention drafted by the Council of Europe).

Many of the general problems of criminalization (precisely defining the criminal act, avoiding overreach and chilling effects on legitimate conduct, keeping up with technological progress) pose themselves in this area, and some of them are especially acute when a legislature sets out to incriminate assaults on the integrity of IT. The following specific problems come to mind:

- (i) Does the progress of ICT lead to new legal interests, and how can they be defined and protected? For example, is there a need to protect "virtual identities" against theft or forgery, and if so, how can that goal be accomplished?
- (ii) How can criminal law keep up with the quick pace of development of information technology and the character and contents of the worldwide web?

(iii) Given the sophisticated and ever-changing character of the interests to be protected, how can criminal laws be sufficiently precise to satisfy the principle of legality and yet avoid glaring loopholes? How can criminal "acts" be defined when all that can be noticed are certain effects whereas the "act" is committed by an automated computer system?

(iv) What role can or should incrimination of conduct play in relation to other means of protecting sensitive ICT interests? According to the *ultima ratio* principle, criminal law should not be employed as the primary means for preserving the integrity of ICT systems. Should criminal laws, for example, apply in addition to effective civil sanctions, e.g., payment of damages for copyright violations? ICT itself provides efficient devices (e.g., encryption, anti-virus and anti-hacking programs, protection against unauthorized download of copyrighted materials) for defending against attacks. This leads to the question whether criminal law should apply only where such devices cannot provide sufficient protection. But one might also think of obliging users by law to install protective programs, and of creating criminal liability for any failure to reasonably protect one's computer against virus infection (because careless users help to spread viruses).

(v) Many legal systems do not generally regard as punishable activity that is merely in preparation of harmful behavior. In the context of ICT criminality, however, the impending harm that can be so grave that certain preparatory measures may be criminalized. For example, some legal systems have criminal provisions against offering or selling (or even possessing?) software especially designed for the commission of internet crime, e.g., for "cracking" passwords or for bypassing download protection. In consonance with the Council of Europe's Cybercrime Convention, some states have also criminalized the sale or purchase of software designed to facilitate the commission of computer fraud. The limits of the legitimate extension of ICT criminality still need to be discussed.

#### (b) Protecting against Crime Committed through ICT

As has been mentioned above, ICT has created a whole new world of opportunities for individuals intending to commit criminal offenses. Criminal legislation may seek to adapt to this development by using specific tools for controlling and sanctioning the abuse of ICT and especially the internet for committing "ordinary" offenses. Since the focus of the questionnaire is not on these legislative measures, they will be mentioned here only briefly.

##### (i) Limiting anonymity

One aspect of the internet that offers opportunities for crime is the protection of anonymity that the web provides. Several measures have been suggested to limit anonymity, so as to enhance the chance of detection and identification of offenders. One (controversial) measure imposed by the European Union is an obligation on access providers to store transfer data for several months in order to make it possible to retrace data transfers back to the computer of origin. Other measures under discussion include limits on the complexity of encryptions and an obligation of computer owners to divulge passwords. Such measures may appear defensible in the context of an ongoing investigation for serious crime, but they necessarily spill over to instances of permissible use of the internet and have the potential of strongly reducing the attractiveness (and thus the profitability) of the net as well as of violating users' legitimate privacy interests.

##### (ii) Controlling content

There is an understandable tendency of legal systems to extend existing criminal prohibitions with regard to written or printed materials (e.g., pornography, incitement to religious or racial hatred, instruction to commit crimes, disclosure of protected state, military or business secrets) to similar materials distributed by means of ICT. This tendency raises a number of specific problems: first, the transnational character of the worldwide web makes it difficult to enforce national standards, and international agreement on the proper scope of restrictions of speech is difficult to achieve. Second, the *ultima ratio* principle raises the issue whether measures short of the imposition of criminal sanctions are at least equally effective. Third, the anonymity of the net leads to the question whether it is possible to extend criminal responsibility for illegal contents to (easily identifiable) providers of internet services, which might reduce the difficulty of piercing the shield of anonymity when attempting to effectively control internet content.

The difference of national interests and standards in prohibiting (or protecting) speech seems to be difficult to overcome (this is an aspect to be treated mainly in Section IV of the Congress) Legal system differ strongly as to (i) what content they regard as harmful or dangerous and (ii) where they draw the line between materials protected by freedom of speech and materials the proliferation or even possession of which will be criminally prosecuted. Beyond the technical issue of the applicability of national criminal laws to materials available on the internet (but presumably "posted" by foreign citizens in foreign countries), these differences create a great impediment to international cooperation in the prosecution of (possible) content offenses. International conventions in this area might resolve that problem, but their drawback is that they tend to maximize criminalisation, because each participating country adds its "pet crimes" to the list of prohibited conduct and there is little political support for retaining breathing space for individual freedom of expression.

Alternatives to criminal prosecution for offensive content are blocking of access to (through the use of software) and deletion of undesirable websites. However, even if access blocking is technically possible it requires cooperation of all nations to be effective, because a block installed by one national agency can easily be circumvented by using an access provided by a foreign firm that does not cooperate with the national agency in question. Deletion, if possible, might be likewise of limited effect because an offending webpage can easily (even automatically) be restored under a different name.

This leads to the issue of making access and/or service providers criminally responsible for maintaining and keeping accessible illegal content. Under this approach, providers would be obliged to “police” and if necessary censor the net. Content providers could be required to either react to complaints about illegal content or even to proactively investigate the contents they provide for prohibited materials. Even if that were technically possible, the normative question arises on what legal basis a (costly) duty to police the net could be imposed on content providers. If one postulates an affirmative legal duty for providers, their criminal liability for breaching this duty could be based on the doctrines of accessorial liability or omission. In that regard, provider liability is to be discussed in Section I on the General Part.

## Section 2: Concept paper and questionnaire

Emilio C. Viano

### (A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with “cyber crime.” This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Emilio C. Viano: [emilio.viano@gmail.com](mailto:emilio.viano@gmail.com)

### (B) Legislative Practices and Legal Concepts

- (1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).
- (2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?
- (3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

### (C) The Specific Cybercrime Offenses

- (1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?
- (2) Are there also negligent offenses in this field?
- (3) If yes, please, provide a list of those offenses.

#### (a) Integrity and functionality of the IT system

##### *1. Illegal access and interception of transmission*

###### *a. Object – system or data?*

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

###### *b. Requirement of infringement of security measures?*

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

##### *2. Data and system interference*

###### *a. Object – protection of system/hardware/data?*

Does your criminal law define “computer and/or electronic data”? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

###### *b. Act – destruction/alteration/rendering inaccessible?*

*i.* Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

*ii.* Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

### 3. Data Forgery

#### a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

#### b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

### 4. Misuse of Devices

#### a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

#### b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under a?

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

#### c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

## (b) Privacy

### 1. Violation of Secrecy of Private Data

#### a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

iii. Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

#### b. Act – illegal use and transfer/distribution?

i. Does the criminal law of your country define the illegal transfer and distribution of private data?

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

#### c. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

### 2. Violation of professional confidentiality

#### a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;
- Their disclosure practices;
- Their professional ethical obligations;
- And whether patients or clients have any control over the disclosure of their personal data?

ii. Which data are specifically protected, if any?

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

b. *Subject – Type of perpetrators?*  
Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

c. *Act – illegal use and transfer/distribution?*  
Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

### 3. *Illegal processing of personal and private data*

#### a. *Object?*

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

#### b. *Subject?*

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

#### c. *Act?*

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply for each category listed below citing the relevant law and its provisions, if available:

1. Illegal collection
2. Illegal use
3. Illegal retention
4. Illegal transfer

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

#### d. *Justification?*

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

### 4. *Identity theft*

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

#### a. *Object*

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

#### b. *Subject*

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

### (c) Protection Against Illegal Content: ICT Related

#### 1. *Object*

##### a. *Child pornography - images of real or virtual children?*

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

ii. In particular, does your criminal law:

- Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:

1. to transmit,
2. make available,
3. export
4. and intentionally access child pornography on the Internet;

- Allow judges to order the deletion of child pornography posted on computer systems in your country;
- Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;
- Criminalize:
  1. Knowingly accessing child pornography on the internet
  2. Transmitting child pornography on the internet
  3. Exporting child pornography on the internet
  4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it...?
    - iii.* Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?
    - iv.* Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?
    - v.* Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?
    - vi.* Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.
    - vii. Mens rea:* To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

*b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)*

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?
2. cyber-bullying?
3. cyber-stalking?
4. cyber-grooming?

*2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)*

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT? Please, cite the relevant law.

1. Fraud
2. Infringement of Intellectual Property IP rights
3. Industrial espionage

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

(f) Non-Compliance Offenses

Does your criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber

systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

(D) Complementary optional information concerning law and practice (including statistics)

- (1) Are cybercrimes included as such in the collection of data on crime in your country?
- (2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.
- (3) Do victimization surveys in your country include questions on cyber-crimes?
- (4) What types of computer crime / computer fraud are most often reported in your country?
- (5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?
- (6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.
- (7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?
- (8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

Forms and Means of Cyber-Crime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)			
Hacking (illegal intrusion into computer systems; theft of information from computer systems)			
Malicious code (worms, viruses, malware and spyware)			
Illegal interception of computer data			
Online commission of intellectual property crimes			
Online trafficking in child pornography			
Intentional damage to computer systems or data			
Others			

- (9) In addition, to the above, if there are there any other forms and means of cyber-crime that have occurred (either frequently or infrequently) in your country, please identify them as well as the frequency with which they occur in the following table:

Forms and Means of Conduct	Occur Frequently	Occur Infrequently

Thank you for your valuable collaboration!

## Annex 1

John A.E. Vervaele

### (1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society (Castells 1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

### (2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

#### 1. The integrity and functionality of the cyber-ICT system (CIA offences)

2. Protection of privacy
3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Annex 2

### The Information Society and Related Crimes

Emilio C. Viano

The modern networked society is highly vulnerable to information-age related deviance and criminal behaviors. Globally, in the past few years, concerns have increased sharply over cyber-security, including the issues of cybercrime or high technology crime, "cyber-war," "cyber-defense," "cyber-terrorism," critical infrastructure protection, and information security. At the same time, growing attention is also being paid to how responses to cyber-security may affect and how they should be balanced with human rights values, such as individual autonomy, privacy, anonymous political speech, freedom of expression and freedom of association, human development goals, including access to knowledge, and economic interests, including innovation, competition, and the protection of trade secrets and other proprietary information. These issues of policy and values also present complex technical issues, such as the issue of "attribution," that is, the extent of the ability to determine the true senders of any message or request for information.

There is no question that the technologies that make the information society possible and functional have become essential tools that have significantly affected various aspects of personal and social lives, ranging from education, business, to cultural and leisure activities. With the widespread use of personal computers and of other electronic devices (iPhone, iPad, iPod, iTunes, etc. ) and technology (Skype, Google Earth, etc.) and high speed internet, various related deviant and criminal behaviors have increased significantly, such as hacking, illegal downloading of music and software programs, and stealing others' passwords or identity.

While the accurate extent and overall cost of cyber deviance is unknown and the estimated cost of it actually varies, there is no question that it is now a global and growing phenomenon.

Consequently, cyber-security has become a major concern of governments and the private sector around the world. There seems to have been a major shift in consciousness, stemming from a variety of sources, including:

- Increased appreciation of how critical the Internet and its resources are in multiple spheres of human endeavor and how many infrastructures and systems are increasingly dependent on Internet connectivity and capacity
- Continuing disclosures of major data breaches at financial institutions, other corporations, government agencies and academic institutions globally
- Continuing releases of malware and the increased sophistication of what is deployed
- Continuing reports of varying levels of governmental accessing, monitoring and filtering (or censorship) Internet use and content
- Unattributed cyber-attacks on key infrastructure, e.g. in Lithuania, Estonia, Georgia and other countries and most recently on a nuclear plant and on a munitions base in Iran. Stuxnet and Duqu used against Iran are considered the world's first 'super weapons' for cyber war.
- Concerns with governmental and corporate espionage
- Increased concern over cybercrime, including online fraud, identity theft, child pornography, theft of intellectual property, and related criminal movement of money and money laundering on the Internet
- Privacy concerns about corporate and governmental data access and the widespread collection, recording and diffusion of private information on practically everyone worldwide

As the reach of the information technology and software continues to grow exponentially among the world's population, and given the apparent lack of adequate user awareness on implementation of security protocols, systems operating on the Internet are often perceived as soft targets to a range of entities. These include criminal enterprises, "hackers" (whether for financial gain or as a challenge), cause-based groups, businesses spying on other businesses, proxies for governments, and governments, including their military and intelligence agencies. Motives for the attacks range from financial gain to the advancement of national security interests to the satisfaction of peer recognition.

Any effort to reach international consensus on cyber-security is likely to expose a range of concerns, which in part flow from different visions of national security, of the role and value of the Internet, of human rights, and of economic policy. Some see cyber-security as having state security at its core, which leads to an emphasis on capabilities to monitor and attribute transmissions and to block

any undesirable content. Others strongly believe that Internet governance (including Internet security) involves an integration and balancing of interests, including not only national security but also human rights and the economic and developmental interests associated with a vibrant, innovative and competitive information society. These differing perspectives manifest themselves in many areas. Even the definition of computer crime is debated and contested.

#### (A) Cybercrime: Terminology and Definition

A cybercrime is a type of crime that involves the abuse of information technology. The term cybercrime covers a series of crimes which range from cyber terrorism to industrial espionage. Some cybercrimes may involve only limited influence of computers and networks while others rely almost entirely on the use of a computer or other electronic device and a network. First, an individual might use a computer or other electronic device to engage in criminal activity. Second, the evidence needed to prove a criminal case might be stored in computerized or electronic form. The law governing use of a computer or electronic device to commit a crime is substantive electronic crime law, because it concerns the scope of substantive conduct that has been criminalized. The law governing the collection of computerized evidence is procedural electronic crime law.

Cybercrime is an extensive phenomenon expressed via an intricate ecosystem of operators, victims and instruments. Over the years, in fact, cybercrime has acquired a hierarchical and international organization, with a genuine "black market" for the commerce of data, tools and skills.

As the instruments have become more streamlined, the expertise required to access the world of cybercrime has been lowered: whereas cybercrimes were once perpetrated by groups of "black hats", today almost anyone with some technical skills can download and use instruments in order to carry out some type of attacks, from anywhere in the world.

Today's cybercrimes are characterized by these two aspects: on the one hand, crimes can take numerous different forms in terms of expertise and attacks; on the other hand there is a series of well-structured schemes and mechanisms that typically characterize organizations and markets focused on profit.

Cybercrime refers to any crime that involves a computer or electronic device (iPhone, iPad, tablet, Blackberry, etc.) and a network where a computer or an electronic device may or may not have played an instrumental part in the commission of the crime. Many of the techniques involve the use of a computer/electronic device and of a network. However, many other techniques have nothing to do with computers other than information stored in text files on the computer's hard drive. Because of the diversity of computer/electronic-related offenses, a narrower definition would be inadequate. The rapid emergence of electronic technologies and software and the exponential expansion of the Internet have spawned a variety of new, technology-specific criminal behaviors that go beyond the category of "computer crimes." The terms "cybercrime" or high technology crime or information and communication technology crime are umbrella names for all crimes involving certain electronic devices and an information and communication network, mostly known today as "the internet." Debating semantically whether an act is a computer crime versus a cybercrime versus a high technology or an information and communication technology crime is not that important. Gaining a better grasp of the problem and of its criminal law implications and response is more important. To combat these new criminal behaviors, many countries have indeed passed specialized legislation.

Experts have had difficulty calculating the damage caused by computer and electronic crimes due to the difficulty in adequately defining them; victims' reluctance to report incidents for fear of embarrassment, losing customer confidence and diminished competitiveness; and the lack of detection.

#### (B) Legal Interests Deserving Criminal Law Protection

The major interests identified in this Section II as deserving of the criminal law protection are:

##### (1) The integrity and functionality of the cyber-Information & Communication Technology (ICT) system (CIA offenses)

Offenses against the confidentiality, integrity, and availability of computer systems (called the "CIA" offenses) constitute the major threat to this primary interest of the ICT system.

##### (2) Protection of privacy

The term "privacy" is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. Philosophical debates concerning definitions of privacy became prominent in the second half of the twentieth century, and are greatly influenced by the development of privacy protection in the law. Some defend privacy as focusing on control over information about oneself; others see it as a broader concept required for human dignity or essential for intimacy; others consider it the value that accords us the ability to control the access others have to us. The earliest calls for explicit recognition of privacy protection in law were in large part motivated by the expanding communication technology. It is clear that many people still view privacy is a valuable interest and realize it is now threatened more than ever by technological

advances. There are massive databases and Internet records of all sorts of information about anyone of us, from individual financial and credit history to medical records, to purchases and Internet searches and communications. Most people do not know what information is stored about them or who has access to it. The ability for others to access and link the databases, with few controls on how they use, share, or exploit the information, makes individual control over information about oneself very challenging. The questionnaire for Section II in great part covers the major types of offenses against privacy.

### (3) Protection of digital personality

Our Digital Personality is the pool of digital information about each one of us available to anyone with the right access, tools and motivation to find it. In the digitized world, it represents each one of us. Increasingly it is the first impression that we make upon others, and first impressions are important.

This phenomenon has grown almost accidentally. There are now many ways through which businesses and ordinary people are creating, using, sharing and storing increasing amounts of personal information.

Business tools are emerging to link the various parts of our Digital Personality together to create comprehensive views of each one of us.

There has been continuing outrage at this invasion of our personal space. Yet we persist in using new digital technologies and willfully post material on ourselves that create even more information for others to find.

Personal information on the internet and social media generally legally belongs to the businesses that hold it. They can manipulate, use, trade and store endless amounts of our personal information and yet we currently have limited legal rights to challenge this situation.

Additionally, as digital technologies become increasingly pervasive, we find ourselves living within ubiquitous intelligent interactive systems. Interacting with them is a complex and time-consuming task that sometimes is difficult for everyone, even Information Technology specialists, and at times impossible for certain groups of people. Although there are many user-centric approaches to deal with this phenomenon, ironically, it seems that the only unnatural part of the digital environment is the real human being. To solve this problem the creation of a context-based digital personality (DP) is being worked on as a proxy between digital surroundings and the final user. DPs will benefit from mobile technologies for context-creation, maintenance and usage; and from semantic technologies for formal decisions and verifications. The DP is conceived as being an electronic alter ego that exists independently of us, having executive powers and carrying our identity when we deal with the electronic world. Using it should simplify everyday interaction between users and digital environments and provide a framework for implementing value-added services for mobile operators.

Pertinent questions in Section II address the major possible violations and exploitation of our digital personality, how to protect it, and how to rebalance this lopsided equation of power over sensitive information about us.

### (4) Protection against illegal content

One could summarize illegal content to be any content, images, code, or software that executes or promotes:

- Malware and malicious code
- Denial-of-service attacks
- Computing viruses
- Cyber stalking
- Fraud and identity theft
- Phishing scams
- Information warfare
- Harassment
- Spam, or the unsolicited sending of bulk email for commercial purposes
- Unauthorized access of licensed or protected software, or other intellectual property.
- Drug trafficking
- Terrorism
- Child pornography, child grooming, and some content inappropriate for minors.

Many jurisdictions place limits on certain speech and ban racist, blasphemous, politically subversive, libelous or slanderous, seditious, or inflammatory material that tends to incite hate crimes.

As a reaction to the actual or potential placement of "illegal" material on the web, government policies concerning censorship of the Internet may be broadly grouped into four categories:

- (a) Government policy to encourage Internet industry self-regulation and end-user voluntary use of filtering/blocking technologies.

In these countries laws of general application apply to illegal Internet content such as child pornography and, in some, incitement to racial hatred.

It is not illegal to make content "unsuitable for minors" available on the Internet, nor must access to it be controlled by a restricted access system. Perhaps all such governments encourage the voluntary use of, and ongoing development of, technologies that enable Internet users to control their own, and their children's, access to content on the Internet (e.g. parental controls).

(b) Criminal law penalties (fines or jail terms) applicable to content providers who make content "unsuitable for minors" available online.

Additionally, in these countries, laws of general application forbid other illegal content, like child pornography.

(c) Government ordered blocking of access to content deemed unsuitable for adults.

Some countries require Internet Service Providers (ISPs) to block material while others only allow restricted access to the Internet through a government controlled access point.

(d) Government prohibition of public access to the Internet.

A number of countries either prohibit general public access to the Internet, or require Internet users to be registered or licensed by a government authority before permitting them restricted access as in (c) above.

In the many countries that have restrictive Internet censorship laws, governmental focus appears to be on prohibiting and/or restricting politically sensitive speech, criticism of the government, etc.

Concerns about access to content on the Internet vary markedly around the world and regulatory policy reflects this. What is illegal in one country is not illegal in others, and what is deemed unsuitable for minors in one country is not in others. However, by and large, child pornography is widely criminalized.

(5) Protection of property (including intellectual property rights)

Intellectual property (IP) refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.

IP is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs. The innovations and creative expressions of indigenous and local communities are also IP, yet because they are "traditional" they may not be fully protected by existing IP systems. Access to, and equitable benefit-sharing in, genetic resources also raise IP questions.

Information and Communications Technology is also widely used to commit traditional crimes like fraud. In our very competitive business world, industrial espionage is reportedly conducted frequently to unjustly obtain competitive advantages.

(6) Protection against acts committed exclusively in the virtual world

Crimes, as traditionally thought of, are committed in the so-called real world, in our shared physical reality. The conduct used to commit such crimes, the circumstances involved in their commission, and the harms that result from their commission all occur in "real" places like public streets or private residences. Consequently, existing criminal law imposes liability and penalties for conduct that results in inflicting bodily harms, like injury to persons or property or the unauthorized taking of another person's property. The modern criminal law insists, as a fundamental premise, that liability be predicated upon some conduct—action or inaction in the face of a duty to act—taken in the external, physical world. It fundamentally rejects that liability can be imposed for incorporeal behaviors such as improper or even criminal thoughts.

At the same time, cyberspace exists along with, but distinct from the physical world. It is a shared conceptual reality, a "virtual world," not a shared physical reality. Since it is not a physical domain, some question whether the current principles of criminal law we employ are adequate to address crimes that exploit the unique advantages of cyberspace. This inadequacy cannot exist unless there are material differences between cybercrimes and "real" crimes as to, for example, the conduct used to commit the offenses that fall into both categories, the circumstances surrounding the commission of the offenses, and the harms that result. Naturally, we should not simply assume that criminal conduct that exploits cyberspace represents an entirely new phenomenon called "cybercrime." It may simply be perpetrators using cyberspace to engage in conduct that has long been outlawed for a long time. The telephone, the telegraph, radio, television etc. have been used to perpetrate frauds, for example. However, fraud has been a crime for centuries. The same is true of homicide, whether committed with a knife, a club, a firearm or poison.

Can there be truly virtual crimes that is offenses whose fundamental elements manifest themselves solely or almost solely in cyberspace? There are legal experts who maintain that traditional criminal law principles can be adapted to include most, if not all, the acts considered cybercrimes. Others, nothing especially the considerable difference between the world of the telephone and that

of the internet, the fact that criminals can cause a much greater harm through the internet than other means, like the telephone, to defraud others and the advantage that they have on traditional criminals in avoiding detection and successful prosecution, favor developing new principles of criminal liability and new laws of cybercrimes.

The international responses to the questions on this issue contained in the Section II questionnaire will provide us with an assessment of the direction criminal law is taking internationally on this issue.

#### (7) Protection of enforcement system (non-compliance offences)

Internet Service Providers (ISPs) possess valuable information that can very useful for the investigation of crimes like subscriber information; internet traffic data (log-files, IP-related data); and content data. It is natural for governments, law enforcement, prosecutors to want to access as much information derived from internet use, web surfing and other transactions as possible. This may collide with constitutional notions of privacy, protection from unreasonable searches and seizures, and forbidding governmental "fishing expeditions."

Another situation that often arises is the control that national governments want to have on the content provided by ISPs to their citizens. There are three primary motives for internet censorship: politics and power, social norms and morals, and security concerns. Protecting intellectual property rights and existing economic interests can also lead to internet censorship. In addition, blocking the networking tools and applications that allow the sharing of information is not infrequent in some countries. Censorship directed at the political opposition is especially frequent in authoritarian and repressive regimes. Some countries block Web sites related to religion and minority groups, often when these movements represent a threat to the ruling regimes. There have been well publicized conflicts and clashes between well known ISPs and the governments of certain countries on this issue. Financial interests related to intellectual property rights can also be a factor justifying drastic governmental intervention.

The questionnaire aims at obtaining information on this wide and complicated issue that reflects different legal traditions (e.g. the concept of *Lèse majesté*), cultural values, and economic priorities.

#### (C) International Approaches

Developing an international paradigm for addressing electronic crime is a challenge, given the global nature of the technology. All nations continue to struggle to define these crimes and develop electronic crime legislation applicable to both domestic and international audiences and situations. Purely domestic solutions are inadequate because cyberspace has no geographic or political boundaries and many electronic systems can be easily and surreptitiously accessed from anywhere in the world. International financial institutions are common targets for electronic fraud and embezzlement schemes. In addition, the development of sophisticated electronic technology has enabled organized crime and terrorist groups to bypass government detection and carry out destructive acts of violence. Even when computer-specific criminal statutes are in place, the rules of evidence in several industrialized countries could continue to hinder prosecutions until they adapt them to electronic crimes. Countries that restrict their political discourse face the problem that the Internet provides a source of "illegal" information that is difficult to regulate. Moreover, what constitutes "acceptable" speech in the various countries on the information super-highway differs greatly, even between Western democracies. Solutions to freedom of expression issues on the Internet have varied widely. Some European countries initially tried to target the Internet service providers (ISPs). Other countries have implemented regulations that criminalize the distribution or consumption via the Internet of "harmful" information, and at times or even permanently limit or disrupt internet access.

Intellectual property crimes are a serious problem in the international arena. International software piracy remains endemic which means that many software applications existing on electronic devices around the world continue to be unpaid-for, illegal copies. In some cases legislation has been enacted to place considerable requirements and consequently to potentially incriminate Internet Service Providers. The problems of data mining, identity fraud, online gambling, child pornography, controlling employees via information technology, privacy violations by social media and search engines, like Facebook and Google, or wireless communications, like iPhones, are attracting considerable attention and concern.

Worldwide, national governments are adopting computer-specific criminal codes that address unauthorized access, violations of privacy rights and manipulation of data. While a number of differences remain, there are significant areas of convergence in various nations' legislation. By defining specific new offenses and penalties, these codes avoid analytical difficulties that arise when general criminal laws are applied to computer crimes. At the same time, however, electronic governmental access to private or business information, bypassing traditional steps of constitutional protections and procedural criminal law, are raising concerns, new and difficult questions and the need to update substantive and procedural criminal law.

International organizations and private corporations are also working to combat ICT crimes by contributing to the drive to harmonize national legislation. Nonetheless, international efforts have been mixed.

(D) The Questionnaire

It is clear that our information society has generated many new problems, challenges and opportunities for criminal law. There is a clear need to expand the frontiers of criminal law and of its application. The protection of privacy and human rights remains a paramount concern. The many areas of intervention mentioned above are appropriate for debate in Section II since they constitute the core of the specific expansion and innovation in substantive criminal law required by the information society that more and more encompasses and even controls not only our lives and activities but also world affairs, international relations and the threat of cyber wars. The accompanying questionnaire for Section II, Special Part, has been designed

to collect relevant information on the response of criminal law to cybercrime in various countries worldwide. The questionnaire is organized around the major interests that have been identified as deserving protection (see above Section C). The questions center around the interests to be protected and the classical criminal law requirements of *actus reus*, *mens rea*, and the penalty envisioned in the law for different types of perpetrators like private persons, public officials, investigators, etc. The questionnaire limits itself to set major markers in the field and allow the National Reporters to contribute information taking into account different legal traditions and varying stages of development of national cybercrime laws. It is hoped that following this scheme of legal interests will facilitate the work of the National Reporters and elicit valuable information on the status of cyber criminal law worldwide. This should be fertile material for the development of resolutions at the Preparatory Colloquium and at the International Congress of the AIDP.

## Section 3: Concept paper and questionnaire

Johannes F. Nijboer

### (A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with “cyber crime.” This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. J.F. Nijboer: [J.F.Nijboer@law.leidenuniv.nl](mailto:J.F.Nijboer@law.leidenuniv.nl)

### (B). General Questions

- (1) Are there current (legal or socio-legal) definitions for applications of IT and ICT within the context of criminal procedure (including forensics)? How are such conceptual definitions reflected in the literature, legislation, court decisions, and relevant practices within the context of the criminal process?
- (2) Are there specific institutions and/or task forces involved in the implementation of ICT within the criminal justice system?
- (3) Are there private (commercial) organisations (companies) that offer ICT related services to the criminal justice system? If so, can you give examples? What limits have to be observed?

### (C) Information and Intelligence: building information positions<sup>1</sup> for law enforcement

- (1) Which ICT-related techniques are used for building information positions for law enforcement agencies?
- (2) To which type of public (e.g. DNA databases) and private (e.g. PNR or financial data such as SWIFT data) databases do law enforcement agencies have access?
- (3) Can techniques labelled as data mining and data matching be applied? If so, can these techniques be used to create profiles of potential perpetrators or risk groups? If so, have special tools been developed for law enforcement agencies?
- (4) Can coercive measures (e.g. interception of telecommunications) be used for building up information positions?
- (5) Which private actors (e.g. internet providers or telecom companies) retain or are obliged to retain information for law enforcement agencies?
- (6) Which private actors can provide or are obliged to provide information to law enforcement agencies?
- (7) Is there judicial control on building information positions?

### (D) ICT in the criminal investigation

- (1) Can law enforcement agencies carry out interception in real time of a) e-traffic data; b) content data?
- (2) Can law enforcement agencies have access to/freeze/search/seize information systems for a) e-traffic data; b) content data?
- (3) Can telecom companies or service providers be obliged to share data with law enforcement agencies? In case of non-compliance, are there any coercive measures or sanctions?
- (4) May law enforcement agencies apply video surveillance? Can they oblige natural or legal persons to cooperate?
- (5) May or must law enforcement agencies apply audio-visual recording of interrogations (suspects, witnesses)?

### (E) ICT and evidence

(The chain of stages: collecting/storing/retaining/producing/presenting/evaluating electronic evidence)

---

<sup>1</sup> Building up information positions is part of the so-called intelligence-led-policing (ILP). ILP can be defined as a conceptual framework of conducting policing as an information-organizing process that allows law enforcement agencies in their preventive and repressive tasks. .

- (1) Are there any rules on evidence that are specific for ICT-related information?
- (2) Are there any rules on integrity (e.g. tampering with or improper processing) and security (e.g. hacking) of ICT-related evidence?
- (3) Are there any rules on admissibility (incl. the principle of procedural legality) of evidence that are specific for ICT-related information?
- (4) Are there any specific rules on discovery and disclosure for ICT-related evidence?
- (5) Are there any special rules for evaluating (probative value) ICT-related evidence?

(F) ICT in the trial stage

- (1) How can or must ICT related evidence be introduced in the trial?
- (2) Can distant interrogations (e.g. by satellite connections) be applied?
- (3) Can digital and virtual techniques be used for the reconstruction of events (killings, traffic accidents)?
- (4) Can audio-visual techniques be used to present evidence at trial (in its simplest form: pictures and sound)?
- (5) Can criminal "paper" case files be replaced by "electronic ones"? Are there any developments towards digitalising of the trial proceedings?

## Annex 1

John A.E. Vervaele

### (1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society (Castells 1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

### (2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

1. The integrity and functionality of the cyber-ICT system (CIA offences)
2. Protection of privacy

3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

(3) References

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Annex 2

## Information society (including information technology) and criminal justice

Johannes F. Nijboer

*Evan Ratliff, an American journalist, tried to vanish in the digital world for a month. He travelled through the United States with a different identity. This experiment was linked to a contest and people 'online' tried to find him. After a month of travelling, trying to be invisible, it seemed impossible in our current information society. Being completely anonymous is not possible due to digital traces. These traces contain for example payments, travelling information and communications.<sup>2</sup>*

*Preamble*

This preparatory document contains a number of observations and reflections that are relevant for the development of a questionnaire for Section III – *criminal procedure*. It has been prepared by Professor Johannes F. Nijboer of the University of Leiden (NL) with the assistance of Mrs. Sanne Kruithof MSc of the University of Leiden. The text was submitted to the AIDP for its preparatory meeting in Siracusa (December 3 and 4, 2010). It is revised for its use as a background document for the draft questionnaire as it stands after the meeting of the rapporteurs in Freiburg im Breisgau (November 20 + 21, 2011).

## (A) Some general considerations

The (post)modern society of today is dramatically different from that of – let us say – 30 years ago. This is true for most countries and regions, even if they are still subject to relatively scarce resources or subject to foreign exploitation of the resources they have. Even in the middle of deserts, high seas, and rainforests mobile telephones and internet can be found. The fast developments in high-tech crime (cybercrime, computer crime)<sup>3</sup> are interrelated to the borderless opportunities of *IT* and *ICT*.<sup>4</sup> But the same applies for the (professional) acts, tools, and instruments within the criminal justice system. Today it appears that even the question of “*hacking*” (which constitutes a crime in most jurisdictions) can be legitimate for police investigations as a means for collecting information. This information may include data that even can be used in evidence.<sup>5</sup>

The last decades of the twentieth century and the beginning of the third millennium have witnessed many new findings and insights. Scientific and technical findings succeed each other with an accelerating speed. Almost all aspects of society are influenced by IT and ICT. It is often difficult to see where developments start, let alone where they stop or are interrupted. Private spheres and public spheres are both affected in a way that makes it steadily more and more difficult to distinguish these two, with for instance an enormous impact for the life of individuals – and the very concept of (social) life as well as the protection of real of privacy.<sup>6</sup> Ratliff (see quotation above) tried to expose this impact on private and public spheres – and the intertwining and mutually interference of these two - with his experiment to vanish for a month. One's very existence can be recorded, registered, and monitored in many ways – without escape. Besides the impact on private and public spheres, the same goes in an institutional sense for the impact on the “*life*” of organizations. This can vary from simple groups, communities and networks or firms to international networks of cooperation, multinational enterprises, non-governmental organizations (NGO's) et cetera.

Part of the complexity of the developments is related to the *convergence of technologies*, for instance in nanotechnology, biotechnology and information technology.<sup>7</sup> They create possibilities and opportunities: on the one side for criminal activities, on the other side for the reactions to this. New forms of criminality, that are related to new technologies can be investigated by applications of techniques that are familiar to the same forms of conduct – e.g. the investigation of internet crime by the use of the internet itself. But science and technique in a broad sense have also an enormous impact on the traditional justice systems. Technological developments and innovations have major consequences for the criminal process. These consequences can theoretical be divided into two groups: alterations and modifications of and additions to existing instruments, procedures et cetera versus (totally) new instruments, procedures et cetera. An example of the first category would be the replacement of paper court files by electronic ones,

<sup>2</sup> <[http://www.wired.com/vanish/2009/11/ff\\_vanish2/](http://www.wired.com/vanish/2009/11/ff_vanish2/)>

<[http://www.marketingfacts.nl/berichten/20100923\\_picnic10\\_evan\\_ratliff\\_wired\\_over\\_digitaal\\_verdwijnen/](http://www.marketingfacts.nl/berichten/20100923_picnic10_evan_ratliff_wired_over_digitaal_verdwijnen/)>

<sup>3</sup> See R.C. van der Hulst & R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders*, Den Haag: WODC, 2008.

<sup>4</sup> Especially within the context of the criminal process the combination of Information Technology and Information and Communication Technology makes it difficult to distinguish both.

<sup>5</sup> See J.J. Oerlemans, Hacken als opsporingsbevoegdheid, *Delikt en Delinkwent* 2011, p. 888-908.

<sup>6</sup> We will come back to this.

<sup>7</sup> See C.J. de Poot, M.P.C. Scheepmaker, Voorwoord, in: *Technology, cognitie en justitie*, Justitiële Verkenningen 2008/1; Boom Juridische Uitgevers, Den Haag, 2008.

an example of the second is the Automatic Number Plate Recognition (ANPR) as it is used to trace, locate and follow cars and individuals.<sup>8</sup>

The types of technologies that draw special attention in the field of the criminal process are the ones that can be used for the detection of persons and acts, the ones that influence human behavior and the ones that help in reconstruction events. Again we give an example of each: refined chemical tests for the detection of biological traces (as part of crime scene investigation) for the first category, electronic surveillance for the second category and computer reconstruction of traffic accidents for the third category. The boundaries between different technologies in applied contexts are not always easy to discern: as said before, there is or can be a convergence. Even the boundary between "real" things and artificial ones is fluent. Is a DNA-fingerprint "*real evidence*"? Or can it better be described as an artifact? And what about statistical information produced by national offices, that most of their data and analyses present in a complex form, with – interlinked - click tabs for the numbers, the graphics, the maps.<sup>9</sup> Within the actual text we will now focus on a part of these numerous developments.

(Post)modern society often is characterized as an "*information society*", because of the widely spread availability and usage of Information and Communication Technology (ICT). The role of ICT is deeply related to scientific and technological developments in general, as generally described before. A few typical features of these developments are (a) the global impact of all kinds of applications, (b) the fast sequence of innovations, (c) the radical changes in the daily work of almost everyone, (d) the transcendent character of changes across natural borders, national borders and limits of time and space, (e) the availability of directly applicable mass data, (f) the loss of traditional monopolies in information, (g) the application of ICT related surveillance devices in different contexts.

A short explanation:

Ad a. Through the combination of integrated computer networks and wireless connections virtually all kind of natural and physical borders can be passed. The very notions of time and place become relative. Within the context of the criminal process one can think of the interrogation of persons (witnesses, suspects) via satellite connections and closed circuit television (CCTV). A DNA-database can be searched within a short period, even by persons in another country (as is the case in the countries that belong to the "Prüm area" within Europe<sup>10</sup>).<sup>11</sup>

Ad b. It is only twenty years ago that elaboration and storage of text by the use of "floppy disks" was an innovation. Today, we might smile when we realize ourselves the speed by which these disks were replaced by CD-ROMs, DVDs and USB-sticks. Sometimes it is argued that it will last for decades before information storages will reach a level of standardization that is equal to the physical "*book*".<sup>12</sup>

Ad c. Due to the endless variety of functions almost everyone has undergone a dramatic change in activities. We buy goods and services on internet (including the check-in for a flight). We inform our contacts from the train or car when we expect to arrive late. But also organizations, including state agencies, have access to data related to virtually anyone. The latter makes our identities vulnerable for purposes of fraud, by the way. Especially the mass storage of information, that can be instantly checked (the running of a DNA-database) is something we will give special attention to in relation to the criminal process, for instance because of the fundamental change in nature or character of the criminal investigation. The already mentioned use of ANPR (combined by the collection of the registered passing of cars at the automatic 'checkpoints') is an example.<sup>13</sup> Turning our focus towards the criminal trial it should be noticed that digital case files – with multiple connection kits or apps – have made their entrance: presentations in a multi-modal way (including "*live*" presentations by audiovisual and digital/virtual reconstructions et cetera).

Ad d. This aspect was already touched upon before. The transnational mobility of persons, goods and services has a multiple impact on our daily life. It also has tremendous consequences in the area of the criminal justice system(s). But it is not only state borders that become less important - it also pertains to natural and physical borders.

Ad e. Like just said about DNA-databases, it can be said that in general enormous quantities of information are available for direct use. Think of internet searches with "machines" like Google. Above this kind of general public availability, many special databases and other "*things*" that contain information are there - most in the commercial sphere, but also in other spheres like (again) the criminal justice system.

<sup>8</sup> Cf. J.F. Nijboer, Signalement: Automatic Number Plate Recognition (ANPR), *Expertise en Recht* 2011/6 (in print).

<sup>9</sup> See P. van den Hoven, *The rubber bands are broken: opening the 'punctualized' European administration of justice, ....*

<sup>10</sup> Austria, the BENELUX countries, France, Germany, Spain

<sup>11</sup> See G. Vermeulen, *Free gathering and movement of evidence in criminal matters in the EU*, Antwerp: Maklu, 2011.

<sup>12</sup> Umberto Eco, Jean-Claude Carrière & Jean-Philippe de Tonnac. *N'espérez pas vous débarrasser des livres*. Grasset & Fasquelle 2009.

<sup>13</sup> And what about the database of the (private) organization that runs the public transport chip-cards in The Netherlands? Or the databases of mobile telephone and internet traffic kept by providers of such services?

Ad f. This is a more complex issue. Of course, it is the case that new markets sometimes spoil older market situations (e.g. the availability of the full content of a book on internet). Traditionally diverse aspects of the state function typically are part of state monopolies. This is the case for aspects of the criminal process too. Here several issues arise, varying from investigative journalism to the "free market" of forensic expertise. Especially in the field of patented technology and science we can observe very complex interrelations between industry and state as well as private agencies (again converging technologies can serve as examples). With some exaggerations we might make a comparison between the "military-industrial complex" in the time of the Cold War and the "forensic-industrial complex" of today.

Ad g) Another feature of today's life is the application of surveillance devices. We find them in the physical world as camera surveillance at gas stations, shopping malls or streets, amusement centres, in busses, trams, metros, trains and ferries, and – last but not least in department stores and in the corridors of hotels (as IMF president Dominique Straus-Kahn found out in New York). But the use of mobile phones and internet can be under surveillance as well: today there is a discussion in The Netherlands about the legality of a high tech content inspection modus used by two phone companies (KPN and Telfort). The discussion concerns the question whether or not this would be only legal for the investigative and security authorities of the state; the companies involved contend that they only look at the nature of the use, not the content of the communications actions of their customers.

Also interesting is the – already mentioned - storage of information by providers and on the chips in devices like public transport chip cards. Often it is very easy to obtain an overview of the journeys of the user during the last month or even longer back in time.

#### (B) Criminal procedure

One of the main areas of the criminal justice system is *fact-finding and evidence* in relation to crime and punishment. It should be noted that many classical crimes can also be committed with the involvement of modern techniques, but that there are also relatively new crimes that are inherently connected to those techniques. From a procedural point of view this is important, since it is the substantive criminal law that denominates the "*investigandum*" and "*probandum*" from the very beginning in the investigation. (As we will see later on the concept of investigation in the traditional sense has become problematic as well.) It goes without saying that new forms of criminality require their own forms of investigation tools and methods. This pertains in special for the domain of ICT crimes (cybercrime<sup>14</sup>).

But there is more, especially in relation to specified databases for instance. The police, the prosecution service, the judiciary, the defense, they all operate in the middle of the information society, and they use the possibilities and opportunities at great length. Although in the context of the criminal process the center of our attention will be on the impact of the information society on the earlier stages of the process, it should be noted that also in the sphere of sentencing and the execution of (namely) prison sentences applied databases are used. In The Netherlands this is the case for the database(s) on imposed sanctions ("*sentencing*")

The availability of new techniques, especially in the ICT world sometimes in combination with other techniques (for example DNA-databases) has dramatically changed the primary processes within the criminal justice system. On one hand the criminal justice system use the new (ICT) technologies available in their daily processes. Take for example the role of paper court files in many countries with a traditional continental system: in high speed many information streams are canalized through electronic systems. Modern courtrooms often are equipped with ICT devices of a rich variety. The application of long distance live connections for a direct interrogation of witnesses or defendants via a satellite is not exceptional any more. On the other hand new techniques influence the investigation and the collection of evidence (in particular within the earlier stages of the process – or even in a broad sense the pre-procedural stage -). We will come back to this in the following paragraph.

#### (C) Intelligence and evidence

Since some decades it is not unusual to distinguish between strategic or tactical information that is available to the police and/or prosecution and information that can be used as evidence. The first kind of information is as "steering" information for the investigation. The mostly used label is "*intelligence*". Such information is never fully disclosed in concrete cases. For a long period the distinction between intelligence and evidence was mainly applied in the Common Law countries. Today, the availability and application is widely spread through non-Common Law countries as well. (This gives – by the way - ground to raise the question whether or not the Common Law concept of "*admissibility*" of evidence within this context could be a fruitful one in non-Common Law jurisdictions.)

In combination with certain kinds of expertise even the existence of "*forensic intelligence*" is a matter of fact. With this context one can think of the combination of information from different databases (DNA-profiles, financial data from the banking branches or tax offices, travel data, license plate numbers, finger prints). In relation to the investigation of organized crime and terrorist cases the boundaries between classical police work and the work of secret services and other types of intelligence services has become fluent.

<sup>14</sup> See U. Sieber, Mastering complexity in the global cyberspace, in M. Delmas-Marty et al. (eds.), *Les chemins de l'harmonisation penale*, Paris 2008, p. 127-202.

The same applies for the sharing of information across national borders. An eye catching example of transnational information exchange on a daily basis is the connection between forensic DNA-databases within a growing number of EU-countries on the basis of the *"Treaty of Prüm"* (and the subsequent EU regulation that has extended its scope).

The existence and the use of enormous amounts of operational information is sometimes referred to as the *"information position"* of investigative and prosecutorial authorities. From this perspective it is *"saillant"* that the presiding Procurator-General of The Netherlands in a television interview indicated that the *"information position"* of the Dutch prosecution service in relation to organized crime was very much ameliorated since about ten years, but that budget cuts cause a limitation to the extent to which indeed criminal investigations could be started (he spoke of about 25% of the known crimes).

Actually this means that there is a world of information or *"intelligence"* available apart from the explicit decisions to enter into a criminal process. There is no a priori reason to assume that in other areas the situation would be very different: the mere fact that many data are available changes the classical picture of investigation. An investigation will often be started on the basis of already existing knowledge. The very decision to act in a concrete case therefore is more than traditionally a matter of choice, it appears. And the choices that are made can be perceived as conscious policies of the authorities. The use of technology and relatively new techniques by the police, but also by private parties such as private protection companies, influences the information position of the police and other investigative or intelligence services compared to earlier times. The possibility comes into existence that technology changes very much the *'beginning'* of the concrete criminal investigation. With the use of technology it is possible to monitor persons or groups and try to reveal criminal acts, even from before they actually happen. Earlier, at least in a more classical view, the criminal acts themselves were the starting point of an investigation. *"Reactivity"* makes steadily more room for *"pro-activity"*.

Besides the influence of technology on (classical) police work, the use of technology has also consequences for the public space. Amongst others Nunn<sup>15</sup> states that the police and other agencies, like private security firms, transforms in – so called- 'surveillance machines'. The use of all kinds of (surveillance) techniques instigates the debate on privacy, we will come back to this later on. Here the notions of the surveillance society and the surveillance state apply.

#### (D) Sources of information (intelligence)

It should not be overseen that in many cases information that is useful for criminal justice purposes is derived from open sources. Especially ICT plays a predominant role. Internet is a big (open) source of information, internet investigation has become an usual tool in many cases. Besides information that can be found on the internet another tool is information which is collected by civilians. A new tool in the Netherlands is a request from the police to civilians to upload their photos and videos from a event made by their mobile phones.

Apart from information from more open sources, it is often possible for the investigating authorities to use information from other more closed government or non-government sources. An – earlier mentioned - example is again the information from public transport (chip)cards or telecommunication-data recorded in databases. Here, it should also be stressed that in most countries there is a vast amount of legislation that obliges providers of ICT services to keep data collected and to make them available to the criminal authorities. It is well known that anti-terror laws have substantially contributed to this state of affairs.<sup>16</sup>

Because of the development of technology, there has been a development of investigative tools too. A few of them have been mentioned earlier. As stated before one of the features of the development of technologies is the loss of traditional monopolies in information. This loss of monopoly is bilateral, on one hand information can be retrieved from more 'open' sources, largely the internet, on the other hand investigative tools are not only available for the government (police), but also for private parties, mainly private security companies. These companies do not exist due to the developments in technology, they have their history back in time when guilds existed. With the grow of the welfare state, (over a long period in the XXth century), the monopoly of the state went bigger, including fields of security and investigation. Recently the welfare state, respectively the monopolies of the state, is/are decreasing. This development gives multiple opportunities for e.g. privately-held security companies. This kind of interrelations fit well into the idea that the state is being transformed into a network state, in which information technology (IT) and information and communication technology (ICT) form the essential organizational principle. This means no less than that the whole concept of the state is changing, including the criminal justice system.

#### (E) The role of the media

Earlier we mentioned the fact that much information comes from open sources. The availability of such sources is connected to the activity of publishers, providers etc. From a wider perspective it seems to be important not to overlook the role of the media. Investigative journalism has become a frequent phenomenon nowadays.

<sup>15</sup> Nunn (2001), 'Police technology in cities – changes and challenges', *Technology in Society* 23, 11-27.

<sup>16</sup> A. Oehmichen, *Terrorism and anti-terror legislation - the terrorised legislator? A comparison of counter-terrorism legislation and its implications on human rights in the legal systems of the United Kingdom, Spain, Germany, and France*, Antwerpen: Intersentia, 2009.

(F) Human rights and fundamental freedoms

It cannot be denied that the societal changes and the related changes in the operation of the criminal justice systems raise many new problems and questions in the area of human rights and fundamental freedoms. Think of the conditions under which biological samples are taken from suspected or other persons in order to produce DNA-profiles to be included in forensic DNA-databases. Or the application of devices for direct interception of private discussions.

Criminal procedure laws traditionally strike balances between human rights and (necessary) limitations to civil freedoms in the interest of public and state interests. Much of the case law of Human Rights Courts, such as the European Court of Human Rights (ECtHR) is related to such issues. In the elaboration of the subject "The Information Society and Criminal Procedure" this area must have major attention. During the last decades most countries have sharpened their legislation for reasons of security and the struggle against terrorism and organized crime in a way that fundamental rights like privacy and physical freedom are sometimes very much limited. There is growing attention in the literature in this field, both from the perspective of Human Rights and of Criminal Procedure. Within the field of human rights the national aspects of the criminal procedure are intertwined with international (global and regional) aspects. Therefore there is a good reason to look closely to the domain that in the work of the AIDP should be covered by the questionnaires and reports in the Sections III and IV.

(G) Some closing remarks

It goes without saying that there is much more to say about the impact of the *"information society"* on the criminal process – especially in relation to ICT and converging techniques. We just mention here the development in facial recognition on the bases of databases of photographs and the use of surveillance cameras. Another important aspect that should be given attention to is the occurrence of false recognitions or identifications (false positives) in the area of surveillance and as a product of the combination of information from different sources. Further we can add the (only at first glance) more *"simple"* error rates in forensic science on the bases of random matches in a DNA database or the risks of change or contamination during the chain of custody of forensic samples (and the use of *"track and trace"* systems to limit that kind of risk). When ever such subjects are looked at, there is almost every time at least one or two connections to ICT as well.

From a more distant point of view, it is good to ask the question whether or not the information society in relation to the *"surveillance state"*, the *"intelligence state"* and the *"database state"* affects the whole basis of the traditional criminal process from its beginning and at the same time in its focus, where the *"investigandum"* and *"probandum"* appears to be more on deviant (and risky?) behavior than on criminal behavior in a stricter sense.

## Section 4: Concept paper and questionnaire

André Klip

### (A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. André Klip: [andre.klip@maastrichtuniversity.nl](mailto:andre.klip@maastrichtuniversity.nl)

### (B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

(2) Can cyber crime do without a determination of the locus delicti in your criminal justice system? Why (not)?

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking, attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

### (C) Substantive criminal law and sanctions

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension?

To what extent do definitions of cyber crime offences contain jurisdictional elements?

To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

Does your national criminal provide for criminal responsibility for (international) corporations/ providers? Does the attribution of responsibility have any jurisdictional implications?

### (D) Cooperation in criminal matters

To what extent do specificities of information technology change the nature of mutual assistance?

(2)(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

(6) Is *self service* (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the (both active and passive) practice in your country?

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

(8) Is your country a party to Passenger Name Record (PNR) (financial transactions, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law. Does your country have an on call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

(12) Does your state participate in Interpol/ Europol/ Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

#### (E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

#### (F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

Is there any other issue related to Information society and international criminal law which currently plays a role in your country and has not been brought up in all the questions before?

## Annex 1

John A.E. Vervaele

### (1) Definition of Information Society? Substantive elements of a definition

No one single information society concept is predominant. Scientists are struggling about definitions and values of the concept and focus on economic, technical, sociological and cultural patterns. Post modern society often is characterized as an "information society", because of the widely spread availability and usage of Information and Communication Technology (ICT). The most common definition of information society lays indeed emphasis on technological innovation. Information processing, storage and transmission have led to the application of information and communication technology (ICT), and related biotechnology and nanotechnology, in virtually all corners of society. The information society is a postindustrial society in which information and knowledge are key-resources and are playing a pivotal role (Bell, 1973 & 1979).

But, information societies are not solely defined by the technological infrastructure in place, but rather as multidimensional phenomena. Bates (1984) pointed out that any information society is a complex web not only of technological infrastructure, but also an economic structure, a pattern of social relations, organizational patterns, and other facets of social organization. So, it is important not to focus only on the technological side, but also on the social attributes of the information society, including the social impact of the information revolution on social organizations, including the criminal justice system.

Moreover, the post modern age of information technology transforms the content, accessibility and utilization of information and knowledge in the social organizations, including the criminal justice system. The relationship between knowledge and order has fundamentally changed. The transformation of communications into instantaneous information-making technology has changed the way society values knowledge. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control. The emergence of a new technological paradigm based on ICT has resulted in a network society (Castells 1996), in which the key social structures and activities are organized around electronically processed information networks. There is an even deeper transformation of political institutions in the network society: the rise of a new form of state (network state) that gradually replaces the nation-states of the industrial era. In this rapidly changing age, the structure of traditional authority is being undermined and replaced by an alternative method of societal control (surveillance society). The transition from the nation-state to the network state is an organizational and political process prompted by the transformation of political management, representation and domination in the conditions of the network society. All these transformations require the diffusion of interactive, multilayered networking as the organizational form of the public sector.

Information and knowledge are key-resources of the information society, affecting the social and political structure of society and state and affecting the function, structure and content of the criminal justice system.

### (2) The interrelatedness of the questionnaires for all four sections

First of all we should use a common working definition. It is clear that computer crime is too narrow for our topic and that "information criminal law or offences related to the information society" is not a well established concept either.

For this reasons we have to use a common definition and a limited focus.

As for as the definition is concerned I do propose to use the concept cyber crime, but with a definition that includes a wide variety of new phenomena and developments.

The common denominator and characteristics features of all cybercrime offences and cybercrime investigation can be found in their relationship to computer systems-computer networks-computer data at the one hand but also to cyber systems-cyber networks-cyber data at the other hand. It goes from the classic computers to the use of the cloud cyber space and cyber databases,

Second, as this is a very broad area, we should focus on the most interesting new areas where our resolutions could produce added value. The outcome of the discussions with the four general rapporteurs is that we will focus on the following legal interests in the field of cybercrime:

1. The integrity and functionality of the cyber-ICT system (CIA offences)
2. Protection of privacy

3. Protection of digital personality
4. Protection against illegal content
5. Protection of property (including intellectual property rights)
6. Protection against acts committed exclusively in the virtual world
7. Protection of enforcement system (non-compliance offences)

### (3) References

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Annex 2

### Concept paper

André Klip

#### (1) Introduction

The fact that modern society has changed into an information society may have dramatic consequences for various aspects of international criminal law. This justifies renewed attention within our association. It is not the first time that the AIDP looked into the topic, albeit quite some years ago, and things have changed.<sup>17</sup> Among other things, the globalisation of our society means that human behaviour may have its effect at many more locations than the place where the initiator of the conduct acted. Google earth, Street View, and Facebook and Hyves make clear to us that for many there is little that others may not be able to see. Big Brother is watching us, what are the implications for international criminal law? Cloud computing raises the question of where data are stored and which legislation applies to it.<sup>18</sup>

In the context of criminal law these extraterritorial effects of conduct may result from the use of certain technologies, such as telecommunication, computers and the web. Hackers may enter a network or an individual computer located in one state from a computer located at the other side of the world. Hate speech may be uttered through twitter, email messages or you tube tapes and have a global expansion. With regard to the material conduct various issues concerning jurisdiction over the conduct and its locus arise.

With regard to the investigations into crimes committed in modern times, the information society leads to new situations and raises new questions. The investigation into an international network for the production of child pornography and the dissemination of its products may require to visit websites, to enter their protected areas, to look into mail boxes, discussion and news groups and to identify the individual IP-addresses of computers.

Also wireless means of communication poses new problems to the law enforcement agencies, because the transmission of data may involve various states or international organisations. The person using a cell phone in one state may converse with a person in another state. However, the satellite(s) transmitting the conversation may be located in other states or in space. What does this mean for the possibilities of intercepting the conversation?

In times in which there are various situations in which it is important to have a certain position of information that will enable the state to prevent or respond to terrorist attacks, states have concluded so called Passenger Name Record agreements. In addition, states have developed (common) databases that may be consulted directly without intervention of the state that supplied the information. For instance, within some states of the European Union, the DNA-database provides for direct consultation whether a new sample matches DNA-profiles already present in the national database and that of the "cooperating" state.

Thus far, despite its presence for quite some decades already, the emergence of cyber crime did not lead to much legislative activity on the international level. The main documents are the Convention on Cybercrime,<sup>19</sup> and its Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.<sup>20</sup> The drafters of the Convention on Cybercrime did relate the necessity of the convention to developments in the society as a whole.<sup>21</sup> What other instruments exist on an international, regional or national level? Despite the fact that states may legislate, technological steps may make the role of private parties increasingly important.

<sup>17</sup> See the general report by Cole Durham, *The Emerging Structures of Criminal Information Law: Tracing the Contours of a New Paradigm*, 64 RIDP 1993, p. 79-117.

<sup>18</sup> See Laviero Buono, *the Global Challenge of Cloud Computing and EU Law*, *Eucrim* 2010, p. 117-124.

<sup>19</sup> Budapest, 23 november 2001, ETS 185, as of 8 November 2010 30 ratifications.

<sup>20</sup> Strasbourg, 28 January 2003, ETS 189, as of 8 November 2010 18 ratifications.

<sup>21</sup> In the preamble to the Convention on Cybercrime the necessity of international legislation in a global information society has been described with the following arguments: "Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters."

## (2) Focus on international aspects

As a thumb rule, relevant for the National Rapporteurs of section 4, it is important that the focus will always be on the international aspects of each segment of their national law. For instance, when rules applicable to the collection and value of evidence are identified, for section 4 it is more important to know how it is determined which state can apply its legislation on it, than to characterise the nature of this evidence in the evidentiary context of the national criminal justice system. The focus of the National Report will always be on the description of the national legal situation in an international context.

## (3) Questions related to jurisdiction over crimes and the locus of the crimes

With the growing importance of the technical developments old legal concepts may have difficulties to keep pace. Whereas in the past it was relatively easy to locate conduct to a specific location (*locus delicti*), it increasingly becomes difficult to locate conduct in cyberspace. States generally have a tendency to prevent negative conflicts of jurisdiction and have increasingly extended the scope of application of their criminal law. They intended to solve the problem by widening jurisdictional principles. Additionally, the cross-border nature of the offence as such has increased multiple jurisdiction.

As a consequence of the practice of widening the extraterritorial application of criminal law, positive conflicts exist by definition. Numerous questions can be raised as a result of it. Should this be prevented? Is this problematic? Does this lead to real problems in practice, or is it in essence an academic problem?<sup>22</sup>

The fact that if all states extend their jurisdiction, automatically concurrent jurisdiction comes into being, raises the question whether certain crimes, for which it may be difficult to find the *locus delicti*, could do without a locus. A key question is thus whether modern crimes can do without jurisdictional principles, which would in essence mean that national criminal law is applicable universally. Is this a road to follow? Should this be limited to certain crimes, for instance crimes, for which there is a conventional basis to criminalise and vest extraterritorial jurisdiction over it,<sup>23</sup> or should this be allowed for all crimes? In the latter situation, national criminal is applicable all over the world, which does seem to be an attractive situation. Could that be solved by allowing for prosecution in cases of a relevant nexus only? To what extent does the concurrent jurisdiction in practice lead to inertia? Does it lead to a *bystander effect*, in which states do not investigate or prosecute crimes committed outside the country, because there are many other states that may have jurisdiction over the offence?

Another way to approach things could be that for certain crimes, for which the *locus delicti* is difficult to find or does imply concurrent jurisdiction, supranational adjudication should be provided. The advantage would be of course that a supranational tribunal would have the power to solve the jurisdictional conflict in a manner binding to the states involved. Additionally, a more specialised tribunal and prosecution could deal with specific forms of transnational crime, which go far beyond the possibilities of national law enforcement authorities. How would an international responsibility for corporations actually work? However, it also means that a further international tribunal might be established, leading to further segregation of the enforcement of the law.

Added to the difficulties in locating the crime is the requirement of double criminality. Most jurisdictional principles, apart from the universality principle, do require that the conduct must also be criminalised according to the law of the place where it was committed. Given the developments of the information society, it is relevant to raise the question whether this requirement still serves a purpose. What is the justification for maintaining a double criminality requirement in the context of the information society of today and for the coming decades? Could we do without it? Which issues are at stake if the rule would be abolished? Could the interests protected by the double criminality rule be safeguarded in other manners?

## (4) Questions related to investigations

Thus far, the rules on the collection of evidence outside the territory have been very straightforward and clear. If law enforcement agencies need information and evidence from elsewhere, they must request foreign authorities to produce it. Police officers of one state may not go without permission to the territory of another state to get what they need. The circumstances currently are

<sup>22</sup> In a recent comparative study commissioned by the Netherlands' Ministry of Justice, Klip and Massa conclude that there are hardly any prosecutions for crimes with a *locus delicti* outside a state's territory. See André Klip and Anne-Sophie Massa, *Communicerende grondslagen voor extraterritoriale rechtsmacht*, Maastricht University 2010 <http://www.wodc.nl/onderzoeksdatabase/vestiging-rechtsmacht.aspx?cp=44&cs=6802>

<sup>23</sup> Such as, e.g. the Convention on Cybercrime.

somewhat different than in the past, because telecommunication networks may enable law enforcement agencies to obtain information and evidence without leaving their own country. A preliminary question is whether it is necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available?

In the context of the information society and obtaining information and evidence for purposes of criminal investigation various situations deserve attention, presumed it is still possible to locate information and evidence: 1. Open information and evidence. This is information which is publicly accessible simply by surfing through the net.

2. Protected information. Information which cannot be publicly accessed, but which may be accessed by hacking. 3. Information and evidence that require to take over a computer or network located in another country.

States continue to have rather strict rules prohibiting the physical presence of foreign law enforcement agents on their territory.<sup>24</sup> Do these rules still apply in the context of modern crimes? Do these rules also apply when law enforcement agents do not physically enter the territory of another state, but do search in networks or computers located in another state. Do the same rules apply and if so, how do they apply? If the rules prohibiting physical presence do not apply, why is that so?

The consequences of not applying the regular rules on mutual assistance in criminal matters are more than symbolic. It would lead to a situation in which assistance from another country is no longer requested and given, but simply obtained through *self service*. This would result in a situation in which traditional grounds for refusal (double criminality, nature of the crime, double jeopardy etc) could no longer be applied. Would it be possible or necessary to reduce the application of grounds for refusal in this area? What are the (theoretical/ practical) consequences of accepting self service as one of the modalities for international assistance in criminal matters?

Once again, it seems that technical possibilities may determine the legal developments and possibilities. This phenomenon may lead to highly interesting theoretical questions about where the primacy for the development of the law should be. However, there are also questions of a more practical legal nature. An example of that relates to the interception of wireless telecommunication. If two persons converse by making use of cell phones, it may involve six states.<sup>25</sup> Should all these states have a say in whether conversations may be intercepted? Or should this be limited to the state that wishes to intercept and why (not)?

Some states and international organisations possess satellites or other devices that enable them to have a clear and detailed picture of every place in the world. Should the law regulate the use for purposes of criminal investigation and prosecution? If so, on which level should this be regulated, national or international and what are the issues at stake?<sup>26</sup>

#### (5) Questions related to classical mutual assistance in criminal matters

To what extent does the information society change the nature of classical mutual assistance?<sup>27</sup> Although some forms of self service may come up and may even be legally accepted, it is unlikely that international mutual legal assistance in criminal matters will completely disappear with the further development of the information society.

The very fact that it has become increasingly simple to speak with persons abroad through audio-visual techniques (skype, videoconference) raises the question whether this should not lead to a higher threshold for extradition for the purposes of prosecution. If the accused is not present in the state that prosecutes him extradition is likely to take place. In light of the serious infringement on the liberty of the accused, the question may be raised whether it should be preferred to conduct the trial via a video-link. Also the presumption of innocence would oppose burdensome extradition. Should we reserve extradition for convicted persons? Do we envisage a virtual court room, in which hearings may take place, whilst nobody is present in the real court room?

Similarly, modern telecommunication creates the possibility of contacting accused, victims and witnesses directly. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why? The very fact that a lot of information is freely accessible anyway and that in many cases persons involved have submitted

<sup>24</sup> Police officers may only enter another country and perform their duties if this finds a basis in a codified international agreement or on the basis of ad hoc permission. The use of coercive measures is generally ruled out. With minor exceptions, such as the apprehension of a fugitive in the case of a cross border hot pursuit. See, e.g. Article 41 of the Convention Implementing the Schengen Agreement.

<sup>25</sup> Gert Vermeulen, *Wederzijdse rechtshulp in strafzaken in de Europese Unie*, dissertation Gent 1999, p. 224-293.

<sup>26</sup> It reminds us of the "telescreens" predicted by George Orwell in his famous novel 1984.

<sup>27</sup> It is interesting to see that the Convention on Cybercrime completely follows the classical principles of international cooperation in criminal matters: a request send by one state to another to render assistance.

the information voluntarily, raises the question why states should still have the power to control whether assistance will be given or not. On the other hand, the view on whether a certain act is within the realm of freedom of speech or a serious crime of breaking confidentiality may differ. Imagine, the US wants certain information in order to investigate the fact that numerous secret and restricted documents concerning the Iraq war have been made available through wikileaks.

What about obligations to retain data on information transmission? Do providers have the obligation to organise their network in such a manner that they may comply with all different and complicated request for assistance from law enforcement agencies of other states? How could this be done with providers not having a seat in the relevant state? Also of a more general nature is, apart from the relevant legislation, the question whether states do have the know-how to deal with crimes committed in the information society. Do law enforcement agencies have the expertise to effectively investigate and enforce the offences in cyberspace?

#### (6) Questions related to obtaining an information position<sup>28</sup>

Especially as part of a package of measures related to combating terrorism states are eager to obtain a good information position in order to prevent terrorist attacks or other crimes from taking place. Given the use of air traffic in the past, as a means of terrorist attacks, states have given priority to have more knowledge on passengers and on freight. Regarding passengers, so called Passenger Name Records agreements have been concluded.<sup>29</sup> Also in other areas, such as financial transactions and visa matters, data are exchanged.

We must be aware of the fact that we are entering here the sphere of privacy law. Whereas on the hand, it should be prevented that the focus of our discussions should be on the elements of the protection of privacy, it is, on the other hand, inevitable that some elements of privacy law will be discussed. National Rapporteurs are requested to focus on the use made for criminal investigations of data submitted or exchanged under PNR (financial transactions or any other) agreements for criminal investigation, not for other purposes such as immigration policy or data retention rules in general. To what extent will the data be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/ correct/ delete information? To what extent can exchanged information be used as evidence?<sup>30</sup>

A further recent development is the establishment of supranational databases and the online consulting of each other's databases. An example of that relates to the EU, in which some Member States have established a mechanism to retrieve data on DNA, licence numbers of vehicles and finger prints directly from another Member State.<sup>31</sup> One of the consequences is, that the state whose data is used, no longer is requested to give information and does not take a decision in individual cases to do so. It also means that grounds for refusal are no longer considered and applied in the initial stage of information exchange.<sup>32</sup> Is this a good development? Within the EU further plans have been developed to create direct access to the criminal records of all Member States.<sup>33</sup> Is that a good thing? Can similar developments be identified in other regions of the world?

#### (7) Questions related to direct enforcement

<sup>28</sup> It is referred to the definition given by Hans Nijboer, General Rapporteur to Section III: "The existence and the use of enormous amounts of operational information is sometimes referred to as the *information position* of investigative and prosecutorial authorities.

<sup>29</sup> The EU concluded agreements with the United States and with Australia on this matter. See <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/431&format=HTML&aged=0&language=EN&guiLanguage=en> Council Decision 2010/16/CFSP/JHA of 30 November 2009 on the signing, on behalf of the European Union, of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, OJ 2010, L 8/11.

<sup>30</sup> In the EU context, a special legal instrument has been adopted regulating the data protection rules in international cooperation in criminal matters. See Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L 350/60.

<sup>31</sup> Council Decision 2009/1023 of 21 September 2009 on the signing, on behalf of the European Union, and on the provisional application of certain provisions of the Agreement between the European Union and Iceland and Norway on the application of certain provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime and Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Annex thereto, OJ 2009, L 353/1; Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008, L 210/1.

<sup>32</sup> However, the relevant legal instruments stipulate that if the information is to be used as evidence, a regular request for international assistance must follow.

<sup>33</sup> Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ 2009, L 93/23.

The almost unlimited possibilities of information technology do raise questions with regard to whether states may directly enforce judgments, notifications, provisional measures etc by making use of information technology, without asking permission of whatever other state.

In a situation in which there is a legal decision that a certain website must close down, because it contains child pornography, hate speech or other illegal material, should it be allowed for law enforcement agencies to hack that site in order to prevent it from further committing crimes?

The notification of judgements, decisions, summons and other legal documents may have legal consequences. Should the law attach these consequences also to notifications sent by information technology?<sup>34</sup> Similarly, should states have the competence to impose upon banks and other financial institutions to confiscate certain financial means in order to keep this for purposes of confiscation of proceeds from crime?

#### (8) Concluding remarks

In sum, at first sight, it seems that the impact of the information society to international criminal law is threefold. The first is that the information society creates a transnational threat for certain legal goods, whilst other may remain unaffected by it. The second is that the information society creates, on the other hand, a tool for criminal justice. The third major impact relates to sovereignty. What does sovereignty mean in our age? Traditionally, the concept of sovereignty gives states a monopoly on the application of criminal law and criminal procedure, based on the territoriality principle. The information society has seriously decreased (or maybe even taken away) the value and importance of territoriality. What does this mean for sovereignty? In sum, the focus of this section is on the extraterritoriality of the conduct, the extraterritoriality of the investigation and the extraterritoriality of the enforcement.

---

<sup>34</sup> In 2010, e.g., the German postal services introduced the electronic Zustellung, equal to a formal notification by an usher.

## MENSAJE DEL PRESIDENTE

*José Luis de la Cuesta*  
*Presidente*

Queridos colegas y amigos, miembros de la Asociación Internacional de Derecho Penal (AIDP-IAPL),

De nuevo, el presente año, tengo el placer de acompañar con mi saludo el boletín cuidadosamente preparado bajo la dirección de la Secretaria General, Katalin Ligeti, para mantener bien informados a todos nuestros miembros de la vida de la Asociación y, en particular, de los acuerdos adoptados en la reunión del Comité Ejecutivo, celebrada en el ISISC (Siracusa, Italia), los días 3 y 4 de diciembre.

La labor de los últimos meses de los órganos directivos de la Asociación ha sido intensa y se ha centrado fundamentalmente en la preparación de los Coloquios preparatorios que, conforme a nuestra metodología congresual, han de elaborar las propuestas de resoluciones a debatir en cada sesión de nuestro XIX Congreso internacional de derecho penal, a celebrar en 2014 en Río de Janeiro (Brasil). A tal fin, y gracias a la hospitalidad de nuestro colega Ulrich Sieber, Director del Instituto Max-Planck de Friburgo de Brisgovia, el Vicepresidente John Vervaele y la Secretaria General pudieron mantener los días 20 y 21 de noviembre una intensa reunión de trabajo con los relatores de las cuatro secciones. De esta reunión salieron los cuatro cuestionarios que, una vez aprobados por el Comité Ejecutivo, se recogen ya en la presente Newsletter (y se publicarán en la Web) para su difusión general y para permitir la elaboración de los correspondientes informes nacionales a presentar en cada Coloquio preparatorio por parte de las personas designadas por cada Grupo nacional.

Nuestro Vicepresidente Jean-François Thony trabaja también con intensidad con las autoridades monegascas a fin de que la Conferencia Mundial, preparada por nuestro Vicepresidente Helmut Epp, pueda tener lugar en Mónaco, a ser posible en otoño de 2012.

En cuanto a los Jóvenes Penalistas, tras la celebración de su Segundo Simposio Internacional (La Rochelle, Francia, 29 de septiembre a 1 de octubre de 2011), preparan en el momento actual la publicación de las actas de esta importante actividad que se culminó con gran éxito.

De estos y otros hitos destacados de la vida de la Asociación trata la presente Carta informativa, que será objeto de difusión general a comienzos del nuevo año. Aprovecho por ello la ocasión para desearles, de todo corazón, unas magníficas fiestas y todo lo mejor para el año 2012.

José Luis de la Cuesta  
Presidente

## LA VIDA DE LA ASOCIACIÓN

*Katalin Ligeti*  
*Secretaría General*

Queridos colegas y amigos,

Durante la segunda mitad de 2011 el Comité Ejecutivo ha seguido trabajando en la aplicación del nuevo programa científico de la AIDP aprobado en junio de 2010. Se pueden encontrar todos los detalles sobre el nuevo programa científico en el apartado elaborado por el vicepresidente John Vervale. Por ello, voy a referirme a las siguientes cuestiones administrativas:

### Nueva sede de la Asociación

Gracias a los esfuerzos del Vicepresidente Thony, la Asociación ya tiene las llaves de las oficinas y se ha firmado el contrato de alquiler formal. La oficina se encuentra en Rue Ferrus (cerca de la Place d'Italie) y cuenta con una sala de reuniones y un lugar donde pueden almacenarse los archivos de la Asociación. También tiene dos plazas de parking. La Asociación cuenta con una importante colección de libros almacenados por el momento en Pau, que deberían ser trasladados a la sede de la Asociación.

### Nuevo folleto de la AIDP

Se han realizado los materiales del nuevo logo y la publicidad de la AIDP con la ayuda de la subvención concedida por el gobierno español. Los folletos de la AIDP se han agotado y se ha dispuesto la impresión de otros 3000 ejemplares (en inglés, francés y español). Carlos Japiassú preparará la versión en portugués del folleto. Los Grupos nacionales interesados en recibir los folletos pueden solicitarlos a la Secretaría de la Asociación.

### Cuestiones diversas

Nuestro Presidente José Luis de la Cuesta ha sido nombrado Doctor Honoris Causa por la Universidad Alexandru Ioan Cuza, por su valiosa aportación al campo del Derecho penal y las ciencias penales. La propuesta fue presentada por la Facultad de Derecho de la Universidad, la más antigua de Rumanía y que incluye en su galería de grandes profesores a Vespasiano V. Pella, Presidente de la AIDP entre 1946 y 1952. La ceremonia de concesión del título tuvo lugar el 28 de octubre en el Aula Magna de la Universidad.

Deseo aprovechar esta oportunidad para informarles de que la reunión del Consejo de Dirección junto con los representantes de los grupos nacionales, así como la reunión del Comité Ejecutivo y del Comité Científico junto con el Comité de redacción de la Revista, se llevará a cabo el 1 y 2 de junio de 2012 en París.

## LAS ACTIVIDADES CIENTÍFICAS DE LA ASOCIACIÓN

*John Vervaele*  
*Vicepresidente*

### Preparación del 19º Congreso Internacional de Derecho Penal y de los cuatro coloquios preparatorios

Continuamos preparando el 19º Congreso Internacional sobre Sociedad de la Información y Justicia Penal.

El 19º Congreso Internacional de Derecho Penal se celebrará en septiembre 2014 y será organizado por el Grupo Nacional de Brasil en cooperación con el socio de la AIDP, el Instituto Brasileño de Ciencias Criminales (IBBCRIM). El Secretario General Adjunto Carlos Japiassú presentará el primer borrador de programa en Junio en París en la reunión del CODIR.

Los Coloquios Preparatorios serán organizados por los grupos nacionales italiano y turco, el Grupo Nacional de Finlandia y el Grupo Nacional Ruso en colaboración con el Congreso Ruso de Derecho Penal. Las fechas de los coloquios preparatorios serán las siguientes:

- Sección 1: Verona (Italia) – 29 noviembre a 1 diciembre 2012.
- Sección 2: Moscú (Rusia) - 24 a 27 abril 2013.
- Sección 3: Antalya (Turquía) - septiembre 2013.
- Sección 4: Helsinki (Finlandia) – la semana del 13 al 15 junio 2013.

Los cuatro relatores generales son:

- Prof. dr. T. Weigend , Sección 1, parte general
- Prof. dr. E. Viano, Sección 2, parte especial
- Prof. dr. H. Nijboer, Sección 3, derecho procesal penal
- Prof. dr. A. Klip, Sección 4, derecho penal internacional

Tras el nombramiento de los relatores generales en la reunión de junio en París, estos elaboraron un proyecto documento de reflexión para su sesión y un proyecto de cuestionario. Estos proyectos fueron discutidos en profundidad en un seminario especial de expertos de dos días en el Instituto Max-Planck de Friburgo, gracias a la generosidad del Prof. U. Sieber. Estuvieron presentes en el seminario de expertos el Prof. U. Sieber, Prof. J. Vervaele, Prof. Katalin Ligeti, dr. Els de Busser, N. von zur Muehlen y los cuatro relatores generales

El resultado del seminario de expertos se ha integrado en el proyecto de documentos de reflexión y los proyectos de cuestionarios por los relatores generales y presentados ante el Comité Ejecutivo en la reunión de Siracusa de diciembre.

En la reunión de Siracusa se aprobaron los resultados finales de las actividades preparatorias, incluida esta newsletter. Esta newsletter, junto con los documentos de reflexión y los cuestionarios de las cuatro sesiones se enviarán a todos los grupos nacionales con la solicitud de que participen activamente en la elaboración de los informes nacionales. Quisiera aprovechar esta oportunidad para agradecer al Prof. Chris Blakesley por la revisión de la versión en inglés de los cuestionarios así como al Prof. Isidoro Blanco por la traducción al español de los textos.

Siguiendo la metodología de los congresos previos, algunos expertos seleccionados deberán trabajar sobre los informes especiales y regionales. El Comité Ejecutivo recomendó los siguientes temas para los informes especiales y regionales:

1. Informe especial:
  - Responsabilidad por violaciones de derechos humanos cometidas mediante las TIC.
  - Defensa de derechos y el uso de las TIC en el proceso penal.
  - Soberanía en el ciberespacio (a preparar por un especialista en Derecho internacional público).
  - Razones de la protección de datos.
2. Informes mundiales y regionales
  - Para la sección 1: Las redes sociales e infracciones cometidas mediante las TI (a preparar por Stanislaw Tosza).
  - Para la sección 2: El Convenio sobre la ciberdelincuencia y desarrollos recientes.

- Para la sección 3: Iniciativas europeas sobre el uso de las TIC en el proceso penal y en la protección de datos (a preparar por Joachim Vogel y Els de Busser).

Se decidió proponer al Comité de Jóvenes Penalistas la designación de relatores para los informes especiales. El Comité de Jóvenes Penalistas puede también proponer nuevos temas para los informes especiales. Igualmente los relatores generales podrán proponer candidatos para la preparación de los informes especiales.

#### Simposio de Jóvenes Penalistas sobre la justicia transicional

Se llevó a cabo en La Rochelle (Francia) entre el 29 de septiembre y 1 de octubre de 2011, el 2º Simposio de Jóvenes Penalistas sobre la justicia transicional. El Simposio fue organizado conjuntamente por el Comité de Jóvenes Penalistas de la AIDP y el Centre d'Études Politiques et juridiques (CEJEP) de la Universidad de La Rochelle (Francia). El Simposio fue patrocinado por la región de Poitou-Charentes, departamento de Charente-Maritime, y el Ayuntamiento de la ciudad de La Rochelle. El Simposio permitió que jóvenes penalistas presentaran sus investigaciones en el ámbito de la justicia transicional. El comité científico seleccionó 21 trabajos que fueron presentados durante las 5 sesiones de trabajo presididas por profesores de derecho penal procedentes de España, Francia e Italia. Participaron en el evento alrededor de 50 jóvenes penalistas de 23 países (de 5 continentes). La sesión inaugural contó con la presencia del Presidente De la Cuesta, quien pronunció un discurso sobre la historia y las actividades de la AIDP. El juez Wolfgang Schomburg pronunció el discurso inaugural. La última sesión concluyó con las observaciones finales de Carla del Ponte, ex fiscal del TPIY y del TPIR.

En la actualidad, el comité científico está editando los trabajos del simposio para ser publicados en 2012.

#### Preparación de la Conferencia Mundial de la AIDP en 2011

Actualmente el Vicepresidente Epp esta negociando la organización de la Conferencia mundial sobre el delito contra el ambiente en Mónaco. La Conferencia podría tener lugar en otoño de 2012.

Si no fuese posible celebrar la Conferencia mundial en Mónaco, podría ser organizada en Manaus (Brasil).

Me gustaría expresar mi profundo pesar por la repentina muerte de nuestro colega y amigo Günter Heine, nombrado relator general de la Conferencia Mundial. Una vez se decida el lugar de la Conferencia Mundial, la AIDP deberá designar lo antes posible al nuevo relator general de la Conferencia Mundial.

#### Conferencias Regionales

El Grupo Nacional de Turquía de la AIDP, junto con el grupo Nacional alemán, organizaron una conferencia regional bajo el título: "Cybercrime: Ein deutsch-türkischer Rechtsdialog". La conferencia tuvo lugar en Estambul los días 13 a 15 de octubre de 2011. El Vicepresidente Vervaele y la Secretaria General Ligeti participaron en la Conferencia.

El Grupo Nacional de Rumania tiene previsto organizar en mayo de 2012 una conferencia regional en Bucarest.

El Presidente Honorario Cherif Bassiouni propuso en la reunión del Consejo de Dirección del ISISC celebrar una importante conferencia de la AIDP en 2012 para celebrar el 40 aniversario del ISISC. Se ofrecerá más información sobre la organización de este evento en la reunión de París de junio.

## LA REVUE Y LAS DEMÁS PUBLICACIONES DE LA ASOCIACIÓN

*Jacques Buisson*  
*Director de la Revue*

### Plan de publicación de la Revue

- RIDP 2011 3-4 : Miscelánea (Redactor Jefe : Isidoro Blanco; Senior: Carlos Japiassu)
- RIDP 2012 1-2 : La justicia negociada (Senior: Thomas Weigend)
- RIDP 2012 3-4 : Derecho a la autorepresentación (senior: Juan-Luis Colomer)
- RIDP 2013 1-2 : Las formas de comisión en los delitos grupo (senior: Thomas Weigend)

### Nouvelles Etudes Pénales (NEP)

La Asociación está planeando publicar las resoluciones de todos los Congresos, incluidas las resoluciones del último Congreso, en los tres idiomas oficiales de la AIDP. Además, el próximo número de las NEP contendrá los textos legales actualizados (estatutos, reglamento interno) de la Asociación.

### Cuestiones diversas

La Asociación apoyará económicamente la publicación del Simposio de los Jóvenes Penalistas de La Rochelle.

## Sección 1: Documento de reflexión y cuestionario

*Thomas Weigend*

### (A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del “Ciberdelito”. Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. Thomas Weigend por email: [thomas.weigend@uni-koeln.de](mailto:thomas.weigend@uni-koeln.de)

### (B) Criminalización

Nótese por favor que en este cuestionario solo son de interés las cuestiones relativas a las características generales de las tipificaciones de las figuras delictivas del ciberdelito. Las cuestiones específicas concernientes a las definiciones de figuras individuales serán objeto de debate en la Sección II del Congreso.

(1) ¿Qué bienes jurídicos específicos se considera que deben ser protegidos por el derecho penal (p.e. integridad de los sistemas procesadores de datos, privacidad de los datos almacenados)?

(2) Por favor, dar ejemplos típicos de leyes penales relativas a

(a) ataques contra sistemas TIC

(b) violación de la privacidad TI

(c) falsedad forgery y manipulación de los datos almacenados digitalmente

(d) distribución de virus de ordenadores

(e) delitos relativos a las identidades virtuales de los usuarios, e.g., forging, sustracción o daño de personalidades virtuales

(f) otras prohibiciones penales innovadoras en el área de las TIC y de internet, e.g., incriminación de la creación y posesión de ciertas imágenes virtuales, violación de derechos de autor en la esfera virtual.

(3) ¿Cómo se define típicamente la conducta criminal (actus reus) en estos delitos (describiendo el acto, el resultado, otros)?  
¿Cómo se define el objeto (“dato”, “escritos”, contenidos)?

(4) ¿Se limita a determinados grupos de autores y/o víctimas la responsabilidad penal por ciertos ciberdelitos?

(5) ¿Se extiende la responsabilidad penal en el área de las TIC a las conductas meramente imprudentes o negligentes?

(6) ¿Hay diferencias específicas entre la definición de los ciberdelitos y los delitos “tradicionales”?

### (C) Técnica legislativa

(1) ¿Hay problemas específicos respecto del principio de legalidad (e.g., vaguedad, remisiones abiertas por parte del tipo penal a otras normativas)?

(2) ¿Cómo evita la legislación los efectos chilling indebidos sobre el uso legítimo de las TIC o de internet?

(3) ¿Cómo evita la legislación penal el peligro de convertirse en obsoleta a la vista del rápida innovación tecnológica? E.g.,

- ¿cómo se tienen en cuenta los cambios en el uso de internet y las redes sociales?

- ¿cómo se adapta la legislación al progreso tecnológico (e.g., mediante la remisión a las normas administrativas)?

## (D) Alcance de la incriminación

- (1) ¿En qué medida la legislación penal alcanza a meros actos preparatorios que conllevan un riesgo de abuso ulterior, e.g., adquisición o tenencia de software que puede ser empleado para “hacking”, “phishing”, fraude de computadoras o elusión de las barreras de protección? ¿En caso afirmativo, la introducción de tales leyes suscitó controversias? ¿Se han hecho esfuerzos legislativos específicos para prevenir la sobrecriminalización?
- (2) ¿En qué medida la mera posesión o tenencia de ciertos datos resulta incriminada? ¿En qué áreas y con base en qué fundamentos? ¿Cómo se define la “posesión” o “tenencia” de datos? ¿Incluye la definición la posesión temporal o el mero visionado?
- (3) En la medida en que la posesión o el favorecimiento del acceso a ciertos datos hayan sido definidas como infracciones penales, ¿la responsabilidad penal se extiende a los proveedores de servicios (e.g., proveedores de acceso o alojamiento)? ¿Cuáles son las exigencias para su responsabilidad, especialmente por lo que se refiere al tipo subjetivo (mens rea)? ¿Están los proveedores obligados al seguimiento y control de la información que suministran o para la que ofrecen acceso? ¿Están obligados a dar información sobre la identidad de los usuarios? ¿Están obligados a impedir el acceso a ciertas informaciones? En caso afirmativo, ¿en qué condiciones y a qué coste? ¿Puede generar responsabilidad penal la violación de esas obligaciones?
- (4) ¿Qué limitaciones generales y, en particular, constitucionales han sido objeto de debate al incriminar conductas relativas a los crímenes concernientes a las TIC y a internet (e.g., libertad de expresión, libertad de Prensa, libertad de asociación, intimidad, “principio de ofensividad”, exigencia de un acto, no mera responsabilidad por resultado (exigencia de mens rea))?
- (5) ¿Prevé la ley sanciones penales específicamente dirigidas a los ciberdelincuentes (e.g., inhabilitación o suspensión temporal para el uso de internet)?

## (E) Alternativas a la criminalización

- (1) ¿Qué papel juega el derecho penal en relación con otras formas de combate del abuso de TIC y de internet? ¿Qué relación existe entre las sanciones civiles y administrativas (pago de los daños, cierre de la empresa, etc.) y las sanciones penales en el área de las TIC?
- (2) ¿Qué medios no penales de combate contra las websites ofensivas se usan/difunden (e.g., cierre de las websites, bloqueo del acceso a las websites)?
- (3) ¿En qué medida se espera de los usuarios de las TIC que apliquen medidas de autoprotección (e.g., encriptación de mensajes, uso de passwords, uso de software de protección)? ¿Se prevén sanciones para la no protección del propio ordenador hasta cierto punto, e.g., usando software antivirus o protegiendo con password el acceso a redes privadas? ¿La ausencia de razonable autoprotección supone un medio de defensa de los acusados por entrada ilícita o por abuso ilícito de la red de otra persona o de sus datos?

## (F) Límites al anonimato

- (1) ¿Hay leyes o reglamentos que obliguen a los proveedores de internet a almacenar los datos personales de los usuarios, incluyendo el historial del uso de internet? ¿Pueden los proveedores ser obligados a suministrar esos datos a la policía?
- (2) ¿Obligan las leyes o reglamentos a los suministradores de servicios de internet al registro de los usuarios con carácter previo al suministro de los servicios?
- (3) ¿Limitan las leyes o reglamentos las posibilidades de encriptación de archivos o mensajes en internet? ¿Pueden los sospechosos ser obligados a disclose los passwords que usan?

## (G) Internacionalización

- (1) ¿Se aplica la legislación doméstica a los datos ingresados en internet desde el extranjero? ¿Hay una exigencia de “doble incriminación” para el ingreso de datos desde el extranjero?
- (2) ¿En qué medida el derecho penal de su país en el área de las TIC y de internet se ha visto influido por los instrumentos jurídicos internacionales?
- (3) ¿Participa su país en debates sobre la armonización de la legislación relativa a los ciberdelitos (como el grupo de expertos intergubernamentales de las NN.UU sobre cibercrimen)?

## (H) Desarrollos futuros

Indique, por favor, las líneas actuales del debate jurídico y legislativo en su país concerniente a los delitos de internet y relativos a la TIC.

## Anexo 1

*John A.E. Vervaele*

### 1. Definición de la Sociedad de la Información? Elementos esenciales de una definición

No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnología de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

### 2. La interrelación de los cuestionarios de las cuatro secciones

En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nueva del ciberespacio y las bases datos cibernéticas.

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del cibercrimen:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID<sup>1</sup>)
2. Protección de la privacidad
3. Protección de la personalidad digital
4. Protección frente a los contenidos ilícitos
5. Protección de la propiedad (incluidos los derechos de propiedad intelectual)
6. Protección contra los actos cometidos exclusivamente en el mundo virtual
7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

### 3. Bibliografía

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Sección 2: Documento de reflexión y cuestionario

Prof. Dr. Emilio Viano

### (A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del “Ciberdelito”. Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas informáticos y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. *El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos informáticos, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.*

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Emilio C. Viano por email: [emilio.viano@gmail.com](mailto:emilio.viano@gmail.com)

### (B) Prácticas legislativas y conceptos jurídicos

(1) ¿Cómo se encuentran reguladas las normas penales relativas a los ciberdelitos en su país? ¿Se recogen en un título unificado o código, o se encuentran en códigos o títulos diversos? (Aportar, por favor, las referencias adecuadas).

(2) ¿Cuál es el impacto de las decisiones judiciales en la formulación del derecho penal relativa a los ciberdelitos?

(3) Para hacer frente a las necesidades y circunstancias cambiantes y para alcanzar nuevos objetivos, algunas leyes sufren frecuentes reformas. Normalmente, tales reformas adoptan la forma de nuevas leyes. En algunos casos esas nuevas leyes, en lugar de modificar simplemente las partes de la ley que precisan ser cambiadas, incluyen las reformas requeridas en un texto consolidado junto con las anteriores reformas. Esta técnica se llama refundición (*recasting*). ¿Es así como las leyes sobre ciberdelitos son actualizadas y adaptadas a las realidades cambiantes en su país? Aportar, por favor, las referencias y citas adecuadas.

### (C) Las infracciones específicas en materia de ciberdelitos

(1) ¿En lo relativo a la *mens rea*, deben las infracciones en materia de ciberdelitos ser dolosas? ¿Se requiere un dolo específico?

(2) ¿Hay también delitos imprudentes en este ámbito?

(3) En caso afirmativo, por favor, aportar una lista de tales delitos.

#### (a) Integridad y funcionalidad del sistema TI

##### 1. Acceso ilegal e interceptación de una transmisión

###### a. Objeto – ¿sistema o datos?

¿Califica su derecho penal como infracción penal la obstaculización grave, ilegítima, del funcionamiento de un ordenador y/o sistema electrónico, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de información o datos de un programa, software o sistema informático?

###### b. ¿Exigencia de infracción de medidas de seguridad?

¿Es un requisito de su derecho penal que el hacker lleve a cabo su conducta de acceso del sistema informático usando uno o más softwares necesarios para saltar las medidas de seguridad y lograr nivel de entrada o un nivel más elevado de acceso?

##### 2. Interferencias con datos y sistemas

###### a. Objeto – ¿protección del sistema/hardware/datos?

¿Define su derecho penal el concepto de “datos electrónicos y/o informáticos”? ¿Incluye esta definición los programas, el software o codificaciones similares? Si tiene una definición, apórtela por favor, así como la referencia a los correspondientes artículos/párrafos de su código.

###### b. Acto – ¿destrucción/alteración/hacer inaccesible?

i. ¿Penaliza su derecho penal el borrado, alteración, conversión en inaccesible, adquisición u otra interferencia similar no autorizada con información o datos de un sistema o programa informático o electrónico?

ii. ¿Penaliza su derecho penal la interceptación no autorizada de cualquier forma o modo de transmisión de información o datos informáticos o electrónicos?

### 3. Falsificación de datos

#### a. Objeto – ¿autenticidad?

¿Define su derecho penal como una infracción penal la introducción, alteración, borrado o supresión no autorizados de datos electrónicos o informáticos que produzca la inautenticidad de los datos con el fin de proteger la autenticidad de los datos susceptible de ser usados o aportados con fines jurídicos? Si dispone de una definición, apórtela por favor con la referencia a los correspondientes artículos/párrafos de su código y/o legislación especial.

#### b. Acto – ¿alteración/borrado?

¿Penaliza su derecho penal como infracción penal la introducción, alteración, borrado o supresión no autorizadas de datos/información electrónica o informática que produzca la inautenticidad de los datos/información con el fin de que sea considerados o aportados a efectos jurídicos como si fueran auténticos? En caso afirmativo, aporte por favor la referencia a los artículos/párrafos correspondientes de su código.

### 4. Uso abusivo de dispositivos

#### a. Objeto – ¿tipo de dispositivos?

¿Penaliza su derecho penal el desarrollo de un “kit de herramientas” de hacker en todo o en parte (e.g. capturadores de contraseñas –password grabbers- y gestores de registro de claves -key loggers-, programas para realización de llamadas gratuitas -blue boxing programs-, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o internet -war-dialers-, software de encriptado -encryption software-, programas de descifrado de contraseñas -program password crackers-, escáneres de vulnerabilidades de seguridad -security vulnerability scanners-, rastreadores de paquetes -packet sniffers- etc.) para el acceso no autorizado a sistemas o transmisiones electrónicas o informáticas?

#### b. Acto – ¿distribución/transferencia pública a otra persona?

i. ¿Penaliza su derecho penal el uso no autorizado de cualquiera de las herramientas de hacker recogidas en el epígrafe i?

ii. ¿Penaliza su derecho penal la distribución pública y/o transferencia a otras partes de la información electrónica hackeada?

#### c. ¿Posesión?

¿Penaliza su derecho penal la posesión de un “kit de herramientas” de hacker en todo o en parte (e.g. capturadores de contraseñas –password grabbers- y gestores de registro de claves -key loggers-, programas para realización de llamadas gratuitas -blue boxing programs-, programas de llamadas automáticas para encontrar vías de acceso a ordenadores y/o internet -war-dialers-, software de encriptado -encryption software-, programas de descifrado de contraseñas -program password crackers-, escáneres de vulnerabilidades de seguridad -security vulnerability scanners-, rastreadores de paquetes -packet sniffers- etc.) para el acceso no autorizado a transmisiones o sistemas electrónicos o informáticos?

## (b) Intimidad

### 1. Violación del carácter secreto de datos privados

#### a. Objeto – ¿tipos de datos privados?

(Datos privados son los datos que pertenecen a la vida privada de la gente pero que no identifican o hacen posible la identificación de una persona, e.g., estado civil, orientación sexual, estado de salud, hábitos o preferencias de compra)

i. ¿Requiere la legislación de su país que los recolectores de datos revelen sus prácticas de información con carácter previo a la recogida de información privada de los consumidores como, por ejemplo, qué información es usada, cómo se recoge y con qué fines, si se compartirá con otros o si los consumidores tendrán control sobre la revelación de sus datos privados?

ii. ¿Requiere la legislación de su país a las empresas y entidades que desarrollen sus negocios en internet que informen a los consumidores sobre la identidad de quien recoge los datos, si el suministro de los datos requeridos es voluntario u obligatorio y los pasos dados por los colectores de los datos para asegurar la confidencialidad, la integridad y la calidad de los datos?

iii. ¿Requiere la legislación de su país a las websites que publiquen su política de privacidad y expliquen cómo usarán la información personal antes de que los consumidores entren en el proceso de compra o en cualquier otra transacción para la que deban suministrar información sensible?

iv. ¿Penaliza el derecho penal de su país el hecho de no suministrar las garantías relativas a la revelación mencionadas más arriba (a.i; a.ii and a.iii)?

#### b. Acto – ¿uso y transferencia/distribución ilegal?

i. ¿Define el derecho penal de su país la transferencia y distribución ilegales de datos privados?

ii. ¿Penaliza el derecho penal de su país el uso, transferencia y/o distribución ilegales de datos privados?

#### c. ¿Justificación?

i. ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución de datos privados?

ii. ¿Qué nivel de necesidad se requiere para una recogida y/o distribución autorizadas (apremiante, importante, razonable, conveniente)?

### 2. Violación de la confidencialidad profesional

#### a. Objeto – ¿tipo de datos privados?

*i.* ¿Requiere la legislación de su país que los profesionales revelen:

- Sus prácticas de recogida y gestión de la información con anterioridad a la recogida de información personal de sus pacientes o clientes:

- Sus prácticas de revelación;

- Sus obligaciones éticas profesionales;

- Y si sus pacientes o clientes tienen control sobre la revelación de sus datos personales?

*ii.* ¿Qué datos se encuentran, en su caso, protegidos de la manera específica?

*iii.* ¿Autoriza o, incluso requiere, el derecho penal de su país al personal sanitario, abogados, sacerdotes, etc. violar la confidencialidad en ciertas situaciones o por ciertas razones legalmente establecidas? ¿En qué condiciones debería hacerse? (e.g. causa razonable que permita ver o creer que hay abuso contra una víctima niño, mujer, persona de edad)?

*b. Sujeto – ¿Tipo de autores?*

¿Identifica el derecho penal de su país las categorías de profesionales sometidos a reglas de confidencialidad específicas?

*c. Acto – ¿uso y transferencia/distribución ilegales?*

¿Qué actos (e.g. recogida ilegal, uso, transferencia y distribución) son específicamente penalizados por la legislación penal de su país?

### 3. Procesamiento ilegal de los datos personales y privados

*a. ¿Objeto?*

¿Penaliza su derecho penal la adquisición, procesamiento, almacenamiento, análisis, manipulación, uso, venta, transferencia, etc. no autorizados e ilegales de datos privados y personales?

*b. ¿Sujeto?*

¿Identifica su derecho penal de manera específica las categorías de personas y entidades incluidas en esta prohibición y sanciones penales?

*c. ¿Acto?*

*i.* ¿Penaliza su derecho penal actos específicos que constituyen el todo o una parte del procesamiento ilegal de datos personales y privados? Responder, para *cada categoría recogida a continuación*, citando el derecho y disposiciones, en su caso, relevantes:

1. Recogida ilegal

2. Uso ilícito

3. Retención ilegal

4. Transferencia ilícita

*ii.* ¿Supone una diferencia el que esos datos personales y privados sean usados, transferidos etc. con fines policiales o de law enforcement?

*d. ¿Justificación?*

*i.* ¿En qué condiciones permite la legislación de su país la recogida, procesamiento, transferencia y distribución autorizados de datos personales y privados?

*ii.* ¿Qué nivel de necesidad se requiere para la recogida y/o distribución autorizadas de datos privados y personales (apremiante, importante, razonable, conveniente)?

### 4. Robo de identidad

*(El robo o usurpación de identidad se produce cuando alguien se apropia de la información personal de otro sin su conocimiento con el fin de cometer un delito de apropiación o de defraudación. El robo de identidad es un medio para la perpetración de esquemas de fraude. Típicamente, se lleva a la víctima a la creencia de que están divulgando información personal sensible para un negocio o entidad legítima, en ocasiones como respuesta a una solicitud por email de actualización de información de facturación o condición de miembro, o como solicitud para un puesto de trabajo o préstamo fraudulento por internet.)*

*a. Objeto*

*i.* ¿Penaliza su derecho penal el robo de identidad? Cite, por favor, el derecho relevante.

*ii.* ¿Proscribe su derecho penal formas específicas de robo de identidad como, por ejemplo, el *phishing*? Se considera el *phishing* como una forma de robo de identidad *online* que utiliza emails con identidad suplantada destinados para atraer a los receptores a *websites* fraudulentas que tratan de engañarlos para que divulguen datos financieros personales como los números de tarjetas de crédito, nombres de usuarios y passwords de cuentas, números de la seguridad social, etc.

*b. Sujeto*

¿Conoce su derecho penal responsabilidad penal ligada a una personalidad digital de una persona o a su Avatar, o a su rol digital en un juego simulado por internet (e.g. Cityville, Farmville, etc.)? Cite por favor las fuentes jurídicas relevantes.

### (c) Protección contra contenido ilegal relacionado con las TIC

1. Objeto

*a. Pornografía infantil - ¿imágenes de niños reales o virtuales?*

*i. ¿Penaliza su derecho penal el uso de internet con objeto de almacenar, acceder y diseminar pornografía infantil? En caso afirmativo, citar las fuentes jurídicas relevantes.*

*ii. En particular, ¿su derecho penal:*

- Crea un nuevo delito que apunta a los delincuentes que usan internet para engañar y explotar niños con fines sexuales? Convierte en delito:

1. transmitir,
2. hacer disponible,
3. exportar
4. e intencionalmente accede a pornografía infantil en Internet;

- Permite a los jueces ordenar el borrado de la pornografía infantil colocada en sistemas informáticos en su país;

- Permite que un juez ordene el embargo de todo material o equipo utilizado en la comisión de un delito de pornografía infantil;

- Penaliza:

1. El acceso a sabiendas a pornografía infantil por internet
2. La transmisión de pornografía infantil por internet
3. Exportar pornografía infantil en internet
4. Poseer pornografía infantil en internet con el fin de, e.g., transmitirla, exportarla...?

*iii. ¿Penaliza su derecho penal la oferta *online* de niños con fines sexuales *via* websites de redes sociales o chats?*

*iv. ¿Es la definición de pornografía infantil de su código penal similar a la recogida en los instrumentos Internacionales (e.g. Directivas UE)?*

*v. ¿Se previene la victimización secundaria de las víctimas de pornografía infantil en su derecho penal? En Estados en los que la prostitución o la aparición en pornografía es un acto castigado por el derecho penal nacional, debería ser posible la no persecución o no imposición de penas por ellas si el menor afectado ha cometido esos actos como resultado de su condición de víctima de explotación sexual o si el menor fue obligado a participar en la pornografía infantil. ¿Es esto lo que su derecho penal contempla?*

*vi. ¿Penaliza su derecho penal la pornografía "infantil virtual"? La pornografía "infantil virtual" no usa niños reales o imágenes de niños reales identificables. ¿Si la imagen no es la de un niño real, sino una combinación de millones de píxeles informáticos realizada por un artista, puede el gobierno de su país prohibir esta creación que se alega es sin víctimas? Citar, por favor, el derecho y/o decisiones judiciales aplicables.*

*vii. Mens rea:* Para ser responsable la persona debería tanto tratar de entrar en un sitio donde la pornografía infantil se encuentra disponible como saber que esas imágenes pueden encontrarse ahí. No debería aplicarse penas a personas que sin advertirlo acceden a sitios que contienen pornografía infantil. ¿Son éstas las exigencias de su derecho penal?

*b. Cualquier otro objeto si la incriminación depende del uso de Tecnologías de la Información y Comunicación (TIC)*

*¿Penaliza su derecho penal las conductas siguientes? Cite, por favor, el derecho relevante.*

1. ¿Creación y uso de verdadero anonimato en el envío y/o recepción de material por las TIC?
2. ¿cyber-bullying?
3. ¿cyber-stalking?
4. ¿cyber-grooming?

*2. Acto – creación/acceso/posesión/transferencia/distribución pública por las TIC (dar ejemplos)*

Citar las leyes específicas que incriminan la creación (incluso aun cuando no se use nunca), el acceso, la posesión (hasta si es sólo privada), la transferencia y la distribución pública por internet y otros medios electrónicos de otros materiales diferentes a los ya mencionados, especialmente debido al uso de la tecnología electrónica o de internet.

(d) Violaciones de la propiedad, incluida la propiedad intelectual, relacionadas con las TIC

*¿Proscribe y penaliza específicamente su derecho penal las conductas siguientes perpetradas por medio del uso de las TIC? Citar, por favor, el derecho relevante.*

1. Defraudación
2. Infracción de los derechos de la propiedad intelectual
3. Espionaje industrial

(e) Criminalización de actos cometidos en el mundo virtual

¿Penaliza su derecho penal la comisión de delitos cometidos en el mundo virtual como, por ejemplo, la pornografía infantil virtual, la violencia virtual, los grafiti virtuales, la ciberdifamación, acoso sexual, acoso laboral, sin afectación de personas reales, sólo mediante representaciones virtuales? Citar por favor el derecho relevante y aportar detalles.

(f) Delitos de Non-compliance

¿Penaliza su derecho penal la no cooperación con las agencias policiales y/o de persecución en el campo del ciberdelito? Los deberes de cooperar pueden consistir en deberes de retener y almacenar información, producir/entregar información solicitada por una orden específica, dar acceso a los sistemas informáticos para la instalación de filtros o dispositivos, etc. ¿Es la infracción del deber de cooperar también susceptible de generar sanciones administrativas? Citar el derecho relevante y aportar detalles.

(D) Información complementaria opcional relativa a la práctica de aplicación de la ley (incluidas estadísticas)

- (1) ¿Se encuentran los ciberdelitos incluidos como tales en la recogida de datos sobre crimen en su país?
- (2) ¿Hay una *website* en su país que suministre datos e información acerca de la frecuencia, gravedad, coste, impacto etc. de los ciberdelitos en su país? En caso "afirmativo", aporte la dirección electrónica de la *website*.
- (3) ¿Las encuestas de victimación de su país incluyen preguntas sobre ciberdelitos?
- (4) ¿Qué tipos de delito informático / fraude informático son los más frecuentemente denunciados en su país?
- (5) ¿Tiene la policía y la fiscalía de su país una unidad de delitos informáticos? En caso afirmativo, ¿cuántos policías/fiscales las integran?
- (6) ¿Su Facultad u otra Facultad de su país ofrece cursos sobre ciberdelito? Aporte por favor la dirección de la web.
- (7) ¿Es el tema del ciberdelito objeto de la formación inicial y/o continua de jueces, fiscales y policía?
- (8) Identifique, por favor, si las siguientes formas y medios de ciberdelincuencia (1) ocurren con frecuencia, (2) ocurren de manera infrecuente, o (3) no han tenido lugar en su país, colocando una "X" en la correspondiente casilla de la tabla siguiente:

Formas y medios de ciberdelincuencia	Ocurre frecuentemente	Ocurre infrecuentemente	No ha ocurrido
Robo de identidad <i>online</i> (incluido el <i>phishing</i> y el tráfico <i>online</i> de información sobre falsa identidad)			
Hacking (intrusión ilegal en sistemas informáticos)			
Código malicioso (gusanos, virus, <i>malware</i> y <i>spyware</i> )			
Intercepción ilegal de datos informáticos			
Comisión <i>online</i> de delitos contra la propiedad intelectual			
Tráfico <i>online</i> de pornografía infantil			
Daño intencional de datos o sistemas informáticos			
Otros			

(9) Adicionalmente a lo anterior, si hay otras formas y medios de ciberdelincuencia que han tenido lugar (tanto si de manera frecuente como infrecuente) en su país, identifíquelas por favor, indicando también la frecuencia de su producción, en la tabla siguiente:

Formas y medios de realización de la conducta	Ocurre frecuentemente	Ocurre de modo infrecuente

¡Gracias por su valiosa colaboración!

## Anexo 1

*John A.E. Vervaele*

### 1. Definición de la Sociedad de la Información? Elementos esenciales de una definición

No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnología de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells 1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

### 2. La interrelación de los cuestionarios de las cuatro secciones

En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nueva del ciberespacio y las bases datos cibernéticas.

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del cibercrimen:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID<sup>1</sup>)
2. Protección de la privacidad
3. Protección de la personalidad digital
4. Protección frente a los contenidos ilícitos
5. Protección de la propiedad (incluidos los derechos de propiedad intelectual)
6. Protección contra los actos cometidos exclusivamente en el mundo virtual
7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

### 3. Bibliografía

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

### Sección 3: Documento de reflexión y cuestionario

*Johannes F. Nijboer*

#### (A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del “Ciberdelito”. Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. Johannes F. Nijboer por email: [J.F.Nijboer@law.leidenuniv.nl](mailto:J.F.Nijboer@law.leidenuniv.nl)

#### (B) Cuestiones Generales

- (1) ¿Existen definiciones (jurídicas o socio-jurídicas) para la aplicación de las TI y de las TIC en el contexto del procedimiento penal (incluida la práctica forense)? ¿Cómo están reflejadas estas definiciones conceptuales en la doctrina científica, la legislación, las decisiones judiciales, y las prácticas pertinentes en el contexto del proceso penal?
- (2) ¿Existen instituciones específicas y / o grupos de trabajo involucrados en la aplicación de las TIC en el sistema penal?
- (3) ¿Existen organizaciones (empresas) privadas (comerciales) que ofrecen servicios relacionados con las TIC en el sistema penal? Si es así, ¿puede dar ejemplos? ¿Qué límites tienen que ser observados?

#### (C) Información e inteligencia: construyendo posiciones de información<sup>35</sup> (information positions) para aplicación de la ley

- (1) ¿Qué técnicas relacionadas con las TIC se utilizan para la construcción de posiciones de información por las agencias de aplicación de la ley?
- (2) ¿A qué tipo de bases de datos públicas (por ejemplo, bases de datos de ADN) y privadas (por ejemplo, el Registro de Nombre de Pasajero o los datos financieros como los datos de SWIFT) tienen acceso las agencias de la aplicación de la ley?
- (3) ¿Pueden aplicarse las técnicas consideradas como minería de datos y comparación de datos? Si es así, ¿pueden utilizarse estas técnicas para crear perfiles de posibles autores o grupos de riesgo? Si es así, ¿se han desarrollado herramientas especiales para las agencias de aplicación de la ley?
- (4) ¿Pueden utilizarse medidas coercitivas (por ejemplo, la interceptación de las telecomunicaciones) para la construcción de posiciones de información?
- (5) ¿Qué actores privados (por ejemplo, proveedores de internet o empresas de telecomunicaciones) conservan o están obligados a conservar información para las agencias de aplicación de la ley?
- (6) ¿Qué actores privados pueden proporcionar o están obligados a proporcionar información a las agencias de aplicación de la ley?
- (7) ¿Existe control judicial de la construcción de posiciones de información?

#### (D) Las TIC en la investigación penal

- (1) ¿Pueden las agencias de aplicación de la ley llevar a cabo intervenciones en tiempo real a) de datos sobre el tráfico, b) sobre el contenido de los datos?
- (2) ¿Pueden las agencias de aplicación de la ley tener acceso / congelar / investigar / secuestrar los sistemas de información sobre: a) datos sobre el tráfico, b) el contenido de los datos?

---

<sup>35</sup> La construcción de las posiciones de información es parte de la denominada actuación policial basada en la inteligencia. Se puede definir la actuación policial basada en la inteligencia como un marco conceptual de llevar a cabo la actividad policial como un proceso de organización de la información que se permite a las agencias de aplicación de la ley en sus tareas preventivas y represivas.

- (3) ¿Se puede obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos con las agencias de aplicación de la ley? En caso de incumplimiento, ¿hay medidas coercitivas o sanciones?
- (4) ¿Pueden las agencias de aplicación de la ley realizar videovigilancia? ¿Pueden obligar a las personas físicas o jurídicas a cooperar?
- (5) ¿Pueden o deben aplicar las agencias de aplicación de la ley grabación audiovisual de los interrogatorios (sospechosos, testigos)?

(E) Las TIC y la prueba

(La cadena de etapas: recogida / almacenamiento / retención / producción / presentación / valoración de la prueba electrónica)

- (1) ¿Existen reglas sobre la prueba específicas para la información relacionada con las TIC?
- (2) ¿Existen reglas sobre la integridad (por ejemplo, manipulación o procesamiento incorrecto) y seguridad (por ejemplo, hacking) de la prueba relativa a las TIC?
- (3) ¿Existen reglas sobre la admisibilidad (incluido el principio de legalidad procesal) de las pruebas que son específicas de la información relacionada con las TIC?
- (4) ¿Existen reglas específicas sobre el descubrimiento y revelación de la prueba relacionada con las TIC?
- (5) ¿Existen reglas especiales para la valoración (valor probatorio) de la prueba relacionada con las TIC?

(F) Las TIC en la etapa de juicio

- (1) Cómo puede o debe introducirse en el juicio la prueba relacionada con las TIC?
- (2) ¿Pueden realizarse interrogatorios a distancia (por ejemplo, conexiones vía satélite)?
- (3) ¿Pueden utilizarse técnicas digitales y virtuales para la reconstrucción de los hechos (asesinatos, accidentes de tráfico)?
- (4) ¿Pueden utilizarse técnicas audiovisuales para presentar pruebas en el juicio (en su forma más simple: imágenes y sonido)?
- (5) ¿Pueden sustituirse los expedientes penales en "papel" por otros electrónicos? ¿Se ha avanzado hacia la digitalización de los documentos del juicio?

## Anexo 1

*John A.E. Vervaele*

### 1. Definición de la Sociedad de la Información? Elementos esenciales de una definición

No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnología de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells 1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

### 2. La interrelación de los cuestionarios de las cuatro secciones

En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nueva del ciberespacio y las bases datos cibernéticas.

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del cibercrimen:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID<sup>1</sup>)
2. Protección de la privacidad
3. Protección de la personalidad digital
4. Protección frente a los contenidos ilícitos
5. Protección de la propiedad (incluidos los derechos de propiedad intelectual)
6. Protección contra los actos cometidos exclusivamente en el mundo virtual
7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

### 3. Bibliografía

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.

## Sección 4: Documento de reflexión y cuestionario

André Klip

### (A) Objeto del cuestionario (ver Anexos 1 2)

Las preguntas de esta Sección tratan generalmente del “Ciberdelito”. Este término se entiende en el sentido de dar cobertura a las conductas criminales que afectan a intereses asociados con el uso de la tecnología de la información y comunicación (TIC), como el funcionamiento adecuado de los sistemas de ordenadores y de internet, la intimidad y la integridad de los datos almacenados o transferidos a o a través de las TIC o la identidad virtual de los usuarios de internet. *El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nube del ciberespacio y las bases datos cibernéticas.*

Si se precisa cualquier aclaración, por favor, contactar con el Relator General, Prof. Dr. André Klip por email: [andre.klip@maastrichtuniversity.nl](mailto:andre.klip@maastrichtuniversity.nl)

### (B) Cuestiones sobre la jurisdicción

- (1)(a) ¿Cómo localiza su país el lugar de comisión de un delito cometido en el ciberespacio?
- (b) ¿Su legislación nacional considera necesario y posible localizar el lugar donde se encuentran la información y las pruebas? ¿Dónde está la información que se puede encontrar en la web? ¿Se encuentra donde el ordenador del usuario está físicamente presente? ¿Allí donde el proveedor de la red tiene su sede (jurídica o de hecho)? ¿Qué proveedor? ¿O es el lugar de la persona que posibilitó la disponibilidad de los datos? Si estas preguntas no se consideran jurídicamente relevantes, por favor, indique por qué.
- (2) ¿En su sistema penal se puede prescindir de la determinación del *locus delicti* en caso de cometerse un ciberdelito? ¿Por qué (no)?
- (3) ¿Qué normas de competencia jurisdiccional se aplican a los ciberdelitos tales como la incitación al odio a través de Internet, hacking, ataques contra los sistemas informáticos, etc? Si su Estado no tiene jurisdicción sobre estos delitos, ¿se considera es esto problemático?
- (4) ¿Su legislación nacional contiene normas relativas a la prevención o a la solución de los conflictos de jurisdicción? ¿Hay alguna práctica sobre ello?
- (5) ¿En su sistema penal se puede prescindir de los principios jurisdiccionales en caso de que se cometa un ciberdelito, lo que en esencia significa que el Derecho penal nacional es de aplicación universal? ¿Debería esto limitarse a ciertos delitos, o estar condicionada a la existencia de un tratado?

### (C) Derecho penal sustantivo y sanciones

- (1) ¿Qué ciberdelitos tipificados en su sistema penal nacional considera usted que tienen una dimensión transnacional?
- (2) ¿En qué medida las definiciones de los ciberdelitos contienen elementos jurisdiccionales?
- (3) ¿Hasta qué punto las reglas de la parte general sobre la comisión, conspiración o cualquier otra forma de participación contienen elementos jurisdiccionales?
- (4) ¿Considera usted que los ciberdelitos constituyen un asunto que un Estado puede regular por sí mismo? Si es así, indique cómo puede hacerlo un Estado. Si no es así, indique por qué no puede hacerlo.
- (5) ¿Su Derecho penal nacional prevé la responsabilidad penal de las empresas / proveedores (internacionales)? ¿Tiene la atribución de responsabilidad implicaciones jurisdiccionales?

### (D) Cooperación en materia penal

- (1) ¿Hasta qué punto las especificidades de la tecnología de la información cambian la naturaleza de la asistencia mutua?
- (2)(a) ¿Se prevé en su país la interceptación de telecomunicaciones (inalámbricas)? ¿Bajo qué condiciones?
- (b) ¿En qué medida es relevante que un proveedor o un satélite puedan estar ubicados fuera de las fronteras del país?
- (c) ¿Su legislación nacional prevé la asistencia judicial mutua en relación a la interceptación de las telecomunicaciones? ¿Ha celebrado su país convenios internacionales al respecto?

- (3) ¿En qué medida las causas generales de denegación se aplican en relación a las investigaciones en Internet y otros medios para acceder a los ordenadores y las redes ubicadas en otros lugares?
- (4) ¿Se exige en su legislación nacional el requisito de la doble incriminación para la cooperación en aquellas situaciones en las que el autor haya causado los efectos desde un Estado en el que se permite la conducta en un Estado en el que se tipifica como delito la conducta?
- (5) ¿Permite su legislación nacional las investigaciones extraterritoriales? ¿Bajo qué condiciones? Por favor, responda tanto a la situación en la que las autoridades nacionales de aplicación de la ley necesitan información, como cuando las autoridades extranjeras necesitan la información disponible en su Estado.
- (6) ¿Se permite el autoservicio (*self service*) (obtención de pruebas en otro Estado sin pedir permiso)? ¿Qué condiciones deben cumplirse para permitir el autoservicio? Por favor, diferenciar la información pública y la protegida. ¿Cuál es la práctica (tanto activa como pasiva) en su país?
- (7) Si es así, ¿se aplica esta legislación también a las búsquedas que se llevan a cabo en la web de acceso público, o en ordenadores que se encuentran fuera del país?
- (8) ¿Es su país parte en acuerdos sobre el Registro de Nombre de Pasajero (PNR) (transacciones financieras, intercambio de ADN, cuestiones de visados o similares)? Por favor especificar y explicar cómo se lleva a cabo el intercambio de datos en la legislación nacional. ¿Tiene su país una llamada unidad que está disponible 24 horas al día y 7 días a la semana para el intercambio de datos? Límitese a las cuestiones relevantes sobre uso de la información para la investigación criminal.
- (9) ¿Hasta qué punto los datos a que se refiere en su respuesta a la pregunta anterior se intercambian para la investigación criminal y cuál es el fundamento jurídico? ¿Hasta qué punto la persona concernida tiene la posibilidad de impedir / corregir / eliminar la información? ¿En qué medida puede esta información ser utilizada como prueba? ¿La ley de su país permite la detección y retirada de un sitio web que contiene información ilegal? ¿Existe alguna una práctica? ¿Desempeña algún papel el sitio del proveedor, propietario del sitio o cualquier otro elemento extranjero?
- (10) ¿Cree usted que es posible un sistema de aplicación internacional para ejecutar las decisiones (por ejemplo, órdenes de suspensión de Internet o inhabilitaciones) en el área de la delincuencia cibernética? ¿Por qué (no)?
- (11) ¿Su país permite la consulta directa de bases de datos nacionales o internacionales que contienen información relevante para las investigaciones criminales (sin solicitud)?
- (12) ¿Participa su país en Interpol / Europol / Eurojust o cualquier otro organismo supranacional que aborde el intercambio de información? ¿Bajo qué condiciones?

#### (E) Aspectos relacionados con los derechos humanos

- (1) ¿Qué normas de derechos humanos o constitucionales son aplicables en el contexto de las investigaciones penales con tecnología de la información? ¿Es relevante para la determinación de las normas aplicables de derechos humanos dónde se considera que se han realizado las investigaciones?
- (2) ¿Cómo se regula la responsabilidad o rendición de cuentas (*accountability*) de su Estado involucrado en la cooperación internacional? Por ejemplo, ¿es su Estado responsable del uso de la información recolectada por otro Estado en violación de las normas internacionales de derechos humanos?

#### (F) Desarrollos futuros

- (1) Las modernas telecomunicaciones ofrecen la posibilidad de contactar directamente con los acusados, víctimas y testigos a través de las fronteras. ¿Se debería permitir eso y, en caso afirmativo, en qué condiciones? Si no es así, ¿se deberían aplicar las reglas clásicas de asistencia mutua (solicitud y respuesta), y por qué?
- (2) ¿Existe algún impedimento legal en su legislación para las audiencias a través de medios audiovisuales (a través de Skype o de otro medio) en casos transnacionales? Si es así ¿cuál? Si no es así, ¿hay alguna práctica?
- (3) ¿Hay alguna otra cuestión relacionada con la sociedad de la información y el Derecho penal internacional que actualmente juega un papel en su país y no ha sido tratado en las preguntas anteriores?

## Anexo 1

*John A.E. Vervaele*

### 1. Definición de la Sociedad de la Información? Elementos esenciales de una definición

No existe un concepto único de sociedad de la información que predomine. La doctrina se esfuerza en la concreción de las definiciones y valores del concepto y se centran en cuestiones económicas, técnicas, sociológicas y culturales. La sociedad post moderna a menudo es caracterizada como una "sociedad de la información", debido a la amplia disponibilidad y uso de la Tecnología de la Información y la Comunicación (TIC). La definición más común de la sociedad de la información pone el énfasis en la innovación tecnológica. El procesamiento, almacenamiento y transmisión de la información han dado lugar a la aplicación de las tecnologías de la información y la comunicación (TIC), y a las relacionadas con la biotecnología y la nanotecnología, en casi todos los rincones de la sociedad. La sociedad de la información es una sociedad postindustrial en la que la información y el conocimiento son los recursos clave y están jugando un papel fundamental (Bell, 1973 y 1979).

Sin embargo, la sociedad de la información no solamente se define por la infraestructura tecnológica, sino más bien como un fenómeno multidimensional. Bates (1984) señaló que cualquier sociedad de la información es una red compleja, no sólo de infraestructura tecnológica, sino también una estructura económica, un patrón de relaciones sociales, modelos de organización y otras facetas de la organización social. Por lo tanto, es importante no centrarse sólo en el aspecto tecnológico, sino también en los atributos sociales de la sociedad de la información, incluido el impacto social de la revolución de la información en las organizaciones sociales, comprendido el sistema de justicia penal.

Por otra parte, la era postmoderna de la tecnología de la información transforma el contenido, la accesibilidad y la utilización de la información y el conocimiento en las organizaciones sociales, incluido el sistema de justicia penal. La relación entre el conocimiento y el orden ha cambiado radicalmente. La transformación de las comunicaciones en tecnología instantánea de información ha cambiado la manera en la que la sociedad valora el conocimiento. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social. La aparición de un nuevo paradigma tecnológico basado en las TIC se ha traducido en una sociedad en red (network society) (Castells 1996), en la que las principales estructuras y actividades sociales se organizan en torno a las redes de información procesada electrónicamente. Existe una transformación aún más profunda de las instituciones políticas en la sociedad en red: el surgimiento de una nueva forma de Estado (Estado en red) que gradualmente sustituye a los Estados-nación de la era industrial. En esta era de rápidos cambios, la estructura de la autoridad tradicional se está debilitando y está siendo sustituida por un método alternativo de control social (sociedad de la vigilancia). La transición del Estado-nación al Estado en red es un proceso organizativo y político impulsado por la transformación de la gestión, representación y dominación política en las condiciones de la sociedad en red. Todas estas transformaciones exigen la difusión de redes interactivas múltiples como la forma de organización del sector público.

La información y el conocimiento son recursos clave de la sociedad de la información, que afectan a la estructura social y política de la sociedad y al Estado y que afectan a la función, estructura y contenido del sistema de justicia penal.

### 2. La interrelación de los cuestionarios de las cuatro secciones

En primer lugar, deberíamos utilizar una definición de trabajo común. Está claro que la referencia a los delitos informáticos es demasiado restrictiva para nuestro tema y que la expresión "derecho penal de la información o delitos relacionados con la sociedad de la información" tampoco tiene un significado claramente fijado.

Por estas razones, tenemos que usar una definición común y un enfoque limitado.

En cuanto a la definición, propongo utilizar el concepto de ciberdelito, pero con una definición que incluye una amplia variedad de nuevos fenómenos y desarrollos.

El denominador común y rasgo característico de todas las figuras de ciberdelitos y de la investigación sobre ciberdelitos puede hallarse en su relación con sistemas, redes y datos de ordenadores, de un lado, y con los sistemas, redes y datos cibernéticos, del otro. El ciberdelito cubre delitos que tienen que ver con los ordenadores en sentido tradicional y también con la nueve del ciberespacio y las bases datos cibernéticas.

En segundo lugar, ya que esta es un área muy amplia, debemos centrarnos en los ámbitos más interesantes en los que nuestras resoluciones puedan aportar valor añadido. El resultado de los debates con los cuatro relatores generales es que nos centremos en los siguientes bienes jurídicos en el ámbito del ciberdelito:

1. La integridad y funcionalidad del sistema de las ciber-TIC (delitos CID<sup>1</sup>)
2. Protección de la privacidad
3. Protección de la personalidad digital
4. Protección frente a los contenidos ilícitos
5. Protección de la propiedad (incluidos los derechos de propiedad intelectual)
6. Protección contra los actos cometidos exclusivamente en el mundo virtual
7. Protección del sistema de cumplimiento de las normas (delitos de incumplimiento [non-compliance offences])

### 3. Bibliografía

Daniel Bell, *The Coming of Post-Industrial Society*, New York, Basic Books , 1976.

Manuel Castells, *The Rise of the Network Society. The Information Age: Economy, Society and Culture Volume 1*. Malden: Blackwell. 2d Edition, 2000

S. Sassen, *The global city* , New York-London, Princeton University Press, 2d edition, 2001.

U.Sieber, *Mastering Complexity in the Global Cyberspace*, in M. Delmas-Marty & M Pieth. *Les chemins de l'harmonisation Pénale*, Paris 2008, 127-202.