# 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

(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[1] 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)?

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

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

(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 Castells1996), 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.*[2]

*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)[3] are interrelated to the borderless opportunities of *IT* and *ICT*.[4] 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.[5]

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.[6] 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.[7] 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,

---

[2] <http://www.wired.com/vanish/2009/11/ff_vanish2/>
<http://www.marketingfacts.nl/berichten/20100923_picnic10_evan_ratliff_wired_over_digitaal_verdwijnen/>

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

[4] Especially within the context of the criminal process the combination of Information Technology and Information and Communication Technology makes it difficult to distinguish both.

[5] See J.J. Oerlemans, Hacken als opsporingsbevoegdheid, *Delikt en Delinkwent* 2011, p. 888-908.

[6] We will come back to this.

[7] 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.[8]
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.[9] 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 al 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[10]).[11]

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*".[12]
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.[13] 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.

---

[8] Cf. J.F. Nijboer, Signalement: Automatic Number Plate Recogniotion (ANPR), *Expertise en Recht* 2011/6 (in print).
[9] See P. van den Hoven, *The rubber bands are broken; opening the 'punctualized' European administration of justice*, …..
[10] Austria, the BENELUX countries, France, Germany, Spain
[11] See G. Vermeulen, *Free gathering and movement of evidence in criminal matters in the EU*, Antwerp: Maklu, 2011.
[12] Umberto Eco, Jean-Claude Carrière & Jean-Philippe de Tonnac. *N'espérez pas vous débarrasser des livres.* Grasset & Fasquelle 2009.
[13] 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[14]).
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

[14] 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.

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. 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[15] 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.[16]
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

[15] Nunn (2001), 'Police technology in cities – changes and challenges', Technology in Society 23, 11-27.
[16] 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.

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.

(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.