(Rio de Janeiro, Brazil, 31st August – 6th September 2014)
International Association of Penal Law (AIDP-IAPL)

SECTION III – CRIMINAL PROCEDURE
INFORMATION SOCIETY AND PENAL LAW

GENERAL REPORT

Lorena BACHMAIER WINTER*
General Rapporteur

Table of Contents
Scope and Objective of the General Report
1. General questions and definitions
2. Information and Intelligence: building information positions for law enforcement
3. ICT in the criminal investigation
4. ICT and evidence
5. ICT in the trial stage

List of Abbreviations
Art./art. Article
CJS Criminal justice system
CoE Council of Europe
CPC Criminal Procedure Code
ECHR European Convention of Human Rights
ECtHR European Court of Human Rights
EU European Union
FISA Foreign Intelligence Surveillance Act
ICT Information and communication technology
ILP Intelligence led policy
IT Information technology
para. Paragraph
TOC Transnational organized crime
UN United Nations
UNODC United Nations Office on Drugs and Crime

Scope and Objective of the General Report
The present general report has been prepared for the XIXth International Congress on Criminal Law that will be held in Rio de Janeiro on 31st August to 6th September 2014 within the AIDP (Association Internationale de Droit Pénal / International Association of Penal Law). The topic of this world congress is focused on the use and impact of ICT in the criminal law and the criminal justice systems, with the aim of understanding and facing the challenges the information society represents for the criminal justice systems. The move towards an information society is irreversible and affects all aspects of society\(^1\). Section III will concentrate on the transformations of criminal investigation and criminal procedure originated by the development of ICTs, trying to give a global overview on how the use of ICT opens the door not only to new solutions and possibilities in the form of investigating, prosecuting and trying criminal offences, but also poses important risks to the protection of human rights, especially the right to privacy and the right to data protection. This general report is based on the comprehensive and excellent national reports received, which provided answers to the questionnaire prepared by the late Prof. Nijboer. These national reports, arrived between January and August

---

* Professor of Jurisdictional and Procedural Law, Complutense University, Madrid, Spain (l.bachmaier@der.ucm.es).
\(^1\) As stated already in 1993 in the White Paper on “Growth, competitiveness and employment. The challenges and ways forward into the 21st Century, known also as the Delors Plan, COM (93) 700, of 5 December 1993.
2013, come from 15 countries: Argentina, Austria, Belgium, Brazil, China, Colombia, Croatia, Finland, Italy, Japan, Netherlands, Sweden, Spain, Turkey and the United States. Additionally, the general report has also taken into account the excellent special reports on EU data protection, EU initiatives on ICTs, ICTs and defence rights, the mass media impact on criminal justice systems (CJS), and the special report on Finland. On behalf of the AIDP and myself, I would like to express my sincere gratitude to all the rapporteurs for their outstanding contributions. In addition to these national and special reports, I have also studied the most relevant UN documents and reports, CoE Conventions and recommendations and other international conventions when preparing the general report. The UNODC Comprehensive study on Cybercrime, published in early 2013, has been especially useful and illustrative to gather information and practices regarding to countries from which we did not have national reports. And, of course, I have also consulted the most significant legal literature, with a special focus on studies published in English.

Despite the efforts to cover the topic of ICT and criminal procedure worldwide, there will likely be gaps in this report, because there are not reports from all national sections and because it is impossible to address every country and every problem arising in every legal system. However, not covering the whole world should not be seen as a shortcoming or a failure. In the first place, because the aim of this general report is only to provide a comparative study to present and analyse the core issues emerging in countries that belong to different legal cultures and have very variegated social and economic circumstances. And in the second place, because my aim has never been to undertake a global study, for comparative studies do not require to address each and every legal system. My purpose has been to highlight problems, to identify trends, to be aware of the challenges and transformations in criminal proceedings due to the growth of cybercrime and the use of ICTs generally—and for this, an overview of several relevant countries is certainly sufficient.

As one of the national reports very accurately states, dealing with ICTs in the criminal justice system is equivalent to dealing with the criminal justice system as a whole, because the use and impact of ICTs is present, to some extent, in every act and every stage of criminal prevention, investigation, prosecution and trial. In fact, ICTs are not exclusively relevant with regard to cybercrime, but have an increasing importance in the context of virtually any type of criminal offence. As indicated in the UNODC Comprehensive Study on Cybercrime, “the growing involvement of electronic evidence in all crime types is likely to revolutionize policing techniques”. Furthermore, J. Nijboer, in the Annex to the questionnaire he prepared for this section, very accurately wrote that “almost all aspects of society are influenced by IT and ICT”; and that “private spheres and public spheres are both affected in a way that it makes it steadily more and more difficult to distinguish these two (...)”. Thus, the use and influence of ICT in the criminal justice systems need to be

---

2 There is no written Spanish national report in the attached CD. Such national report should have been written by me but, due to time constraints, I preferred to concentrate on the general report, rather than writing separately on the situation of ICTs and criminal procedure in Spain. However, the Spanish legal framework and practice have been taken into account when writing the general report.

3 The authors of the national reports are: Javier de Luca et al (Argentina), Farsam Salimi (Austria), Daniel De Wolf (Belgium), Fauzi H. Choukr and Coriolano Almeira (Brazil), Song Yinghui et al. (China), (Colombia), Elizabeta Ivcevic (Croatia), Helena Vihriälä (Finland), Giulio Illuminati (Italy), Tatsuhiko Inatani (Japan), Tijs Kooijmans and Paul Mevis (The Netherlands), Serap Keskin Kiziroglu et al (Turkey), (Sweden), and Stephen Thaman (USA).


5 This study is available at: http://www.unodc.org/documents/organized-crime/UNODC_CCPDJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

6 See the Dutch report, point 1: “Introduction”. In the same sense, M. Simonato, in the special report “Defence rights and the use of information technology in criminal procedure”, p.1. This report covers almost all the aspects addressed in this general report, as the issue of the defence rights is relevant in every stage of the proceedings and with regard to the use of every measure that uses ICTs, and as the author puts it, ICTs in general have strengthened the position of the prosecution and therefore the use of ICTs challenge the position of the defender under the principles of equality of arms.
addressed by scholars at a global level because: 1) it is essential to all criminal proceedings; 2) it is evolving more rapidly than the legal responses the legislator is able to provide; 3) it has a deep impact on the sphere of human rights.

However, it has to be noted that this section of the AIDP—and therefore this general report—deals with ICT and criminal procedure. It might sound redundant to remember this, but it is essential to bear in mind that our main interest is to focus on the impact of the ICT in the CJSs and not in the field of security and espionage. Both areas are not clearly separated, and the borderline between both more than often tends to get blurred. This will require that we deal with the possible transfer of information gathered for security reasons into the criminal procedure—or, in other words, with the admissibility of such information as evidence for adjudicating purposes. In any event, our aim is not to assess the security policies undertaken by some countries, the increasing role of the so-called cyberimperialism, the different aspects of the development of the surveillance state and the assessment of the ethical behaviour of some of the intelligence agencies worldwide. In simpler words, this report is not about the activities of the National Security Agency (NSA) in the USA, the leaks of information revealed by insiders and the massive intrusion in the privacy of the communications of the citizens by some governments using very sophisticated technology, justifying such encroachment of human rights on threats against national or international security. This does not mean that all these methods for gathering information are not relevant in our study. I only want to underline that our aim is not to evaluate, analyse or criticize the intelligence services in general, and how they proceed or abuse their powers, but to concentrate on criminal investigation, prosecution and procedure. Thus, for example, rather than analysing all the devices the governments use to eavesdrop, our aim will be to examine how this information may flow into the criminal procedure, and to explore mechanisms to prevent that such information can be used in an unfettered and illegal fashion to apply criminal sanctions against the citizens.

This general report follows the structure of the questionnaire sent to the national sections, which contained 25 questions, divided in five sections:

1) General questions and definitions.
2) Building information positions, which tries to address the use of ICT in gathering information by law enforcement agents within a preventive or proactive setting.
3) The role and usage of ICT within the criminal investigation—which is, in my view, the core part of the study and has ended up also being the most extensive part in the proposed draft resolution.
4) The role of the ICT and the evidence in the criminal proceedings. In this section the questionnaire addressed the different stages of evidence: gathering, storing, retaining, presenting, admitting and assessing evidence.
5) The use of ICT at the trial stage.

There are slight overlaps between sections 3, 4 and 5. Therefore, I decided to study the issues of gathering, retaining and storing of electronic evidence under section 3; and the presentation of evidence and the use of ICT during trial within section 5. Section 4 is focussed on the issue of the admissibility and evaluation of evidence. The questionnaire did not include questions on the use of ICTs in the post-trial stage, and hence this issue is not covered in this report, despite its undoubted importance in the practice of execution of judgments.

Before beginning the full report, it is useful to advance some preliminary conclusions that can be drawn from it:

1) There is need for an effective legal framework for ICT investigative measures with an appropriate balance between investigative powers and respect for individual rights, in particular the right to privacy. Many of the ICT measures are carried out on the basis of general rules on search and seizure, which is not appropriate.
2) ICTs are widely used in building up information positions as well as for criminal investigation. Most countries however do not regulate the powers of law enforcement authorities in the preventive stage. Moreover, the transfer of data from the preventive field to the criminal proceedings should be very clearly regulated and mechanisms and controls should be in place to avoid the illegal transfer of such elements.

7 On this, regarding the situation of the USA, before and after the 11-S attacks, see J. Vervaele, “Medidas de investigación de carácter proactivo y uso de información de inteligencia en el proceso penal”, in El proceso penal en la sociedad de la información. Las nuevas tecnologías para investigar el delito, Madrid, 2012, pp. 29-85, p.39 ff.
3) Well-defined rules and protocols on the storing and granting the integrity of digital and electronic evidence shall be elaborated. The defendant should have the opportunity to test the integrity of computer related evidence.

4) The access to databases should be subject to stricter controls, not only at the investigative but also at the preventive stage. Mechanisms to trace which database was accessed, for which purpose and by whom, should be established.

5) Every citizen whose privacy has been encroached upon should be informed of it.

1. General Questions

This section is aimed at providing an overview on the definitions of terms and the institutions involved in the use of ICT in the CJS. Certainly for the substantive criminal law it is important to clarify what cybercrime is and what its elements are, but such definition is equally relevant for the criminal procedure and the criminal justice system in general. Of course, for a common understanding and for a comparative analysis, the agreement on certain definitions will facilitate the work—for example, what is considered an electronic communication or stored personal data. However, what is undeniably essential for assessing the impact of ICTs in the criminal justice system is to know the tools that are used, their role in each of the stages of the criminal procedure, and—this is crucial—how far and under what conditions those data obtained or stored using ICTs can be admissible as evidence. It is unclear if establishing definitions regarding ICTs and criminal procedure might be even convenient, because, as the Belgian report indicates, some definitions could have an adverse impact due to the rapid development of the technology.

(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?

None of the analysed countries defines precisely the meaning of “information society” or contains a specific definition of ICT tools, techniques, mechanisms or measures within the criminal proceedings. In general, the concepts of electronic networks, computer systems, traffic data, content data, forensic tools, etc. are taken from the general ICT language, from international conventions or from the substantive criminal law regulating cybercrime. Within the EU the definitions of electronic communications, computer data, cyber networks, traffic data, content data, service provider, etc. are found in the relevant EU directives, and also borrowed from international conventions such as the Budapest Convention on Cybercrime of 2001. The 2002 EU Directive on privacy and electronic communications defines in its 2 important concepts related to the ICT communications. Although the Directive precisely states that those definitions are included for the Directive purposes, they may be used also within the criminal law procedure. Art. 2 of this EU Directive of 2002 reads:

“Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) shall apply. The following definitions shall also apply:

8 Report of Belgium, question B (1).
9 For example the Data Retention Directive 2006/24/CE in it’s art. 2.2 includes definitions for following concepts:
(a) ‘data’ means traffic data and location data and the related data necessary to identify the subscriber or user;
(b) ‘user’ means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;
(c) ‘telephone service’ means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);
(d) ‘user ID’ means a unique identifier allocated to persons when they subscribe to or register with an internet access service or internet communications service;
(e) ‘cell ID’ means the identity of the cell from which a mobile telephony call originated or in which it terminated;
(f) ‘unsuccessful call attempt’ means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.
(a) "user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;
(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;
(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;
(d) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
(e) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;
(f) "consent" by a user or subscriber corresponds to the data subject's consent in Directive 95/46/EC;
(g) "value added service" means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;
(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

It could be assumed that these definitions are also used in the field of substantive criminal law in the EU countries, but we have no evidence of this.

Exceptionally, the codes of criminal procedure of some countries include some partial definitions or define certain concepts, including definitions and/or rules on for example “computer systems” (Belgium), “information system” (Turkey), digital data processing (Austria, Automationsunterstützte Datenverarbeitung) or electronic evidence and electronic document (Croatia11, Colombia within civil proceedings). Electronic evidence is generally defined as material that exists in electronic or digital form12, but another survey conducted in sixteen European countries revealed that none of them provided for a real definition of digital evidence13. Belgium also adopts a very general and “neutral” definition that covers the use of any kind of ICTs: “every system that allows the storage, processing or transmission of data”.

The USA passed very early special legislation on electronic communications, mainly through the Electronic Communications Privacy Act (ECPA) of 1986, which amended the pre-existing rules on wire tapping, the so called Title III of the Omnibus Crime Control and the Safe Streets Act of 1968. For example, definitions of “electronic communication” and “interception” were included in the USA legal system. According to the national report, “electronic communication” includes “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system”, while “interception” include “eavesdropping contemporaneous with the transmission of communications”, but neither the accessing of stored private e-mail sent to a service provider which has not yet been retrieved, nor the recording of an instant message. Such definitions, while they may clarify the scope of application of the law, have also caused problems of interpretation, for example with regard to the “interception” of e-mails: technically, an e-mail can only be “intercepted” as a communication during those seconds or milliseconds before the sent mail is stored in any temporary location. This raised the question if the “interception” of e-mails should only be allowed under the rules for searching stored data, or if those stored data could be considered “in transmission” until they are retrieved by the recipient, in which case

11 Art. 202, para. 32 CPC: “electronic (digital) evidence means data that was collected as evidence in an electronic (digital) form”, however the Code states also that electronic evidence is not a type of evidence, but a “medium on which the evidence is stored (art. 331 CPC). See the report of Croatia, p.2.
12 UNODC Comprehensive Study on Cybercrime, p. 157.
the rules on interception of communications should apply. We will see that similar problems are found in other legal systems, especially because traditional concepts created for communication or for searches have not been adequately adapted to the new ICT reality and the extensive use of electronic communications.

In general, the criminal procedure provides for scattered legal provisions on different aspects of ICT: only single definitions of ICT investigate measures and requisites for the use of some ICTs for investigation purposes, are found. We should question ourselves if common definitions of ICT related concepts are as necessary within the criminal procedure as they are in the substantive criminal law\textsuperscript{14}. Nevertheless, the appearance and increasing role played by new kinds of data\textsuperscript{15} provided by the use of diverse ICTs—for example, geo-location devices, internet searchers, automatic number plate recognition, chips attached to goods, thermal imaging technology, surveillance cameras, and all types of software tools—have clearly changed the investigation of crimes and present new challenges for the traditional rules on investigative measures and on evidence.

A certain harmonization of the meaning, scope and requirements of ICT investigative measures would be highly desirable. The same applies to terms like subscriber data, meta-data or envelope data, content data and traffic data, and it would be very useful to agree on which of them can be considered “data at rest” and “data in transit”,\textsuperscript{16} as the definition of these concepts will determine which is the investigative measure to be used. This is especially necessary for comparative studies as well as for international cooperation in criminal matters—no doubt the use of the same terms for the same ICT related investigative acts, and an agreement on the meaning of electronic evidence, would facilitate international cooperation and the admissibility of evidence obtained abroad. If we underscore here the importance of definitions and harmonisation in transnational criminal investigations, is because the use of ICTs has facilitated the growth of transnational criminality and thus the need for expeditious execution of judicial cooperation requests. Moreover, even if a crime is committed in the territory of one single state, relevant data might be stored in servers located abroad, or even in the cloud\textsuperscript{17}, posing therefore new challenges to the obtaining of evidence abroad, with implications on the extraterritorial powers and the respect of sovereignty. Finally, for the correct understanding of the relationship of ICT and criminal procedure it is essential to underline that its use and significance goes far beyond the context of cybercrime or computer related investigations and proceedings.

\textbf{(2) Are there specific institutions and/or task forces involved in the implementation of ICT within the criminal justice system?}

The expansion of the use of sophisticated ICTs in the commission of criminal offences represents a continuous challenge for law enforcement and prosecuting authorities that need to keep abreast of all technological innovations, not only to detect those new forms of crime but also to be able to collect evidence for its prosecution. Within the CoE landscape, Recommendation No. R(95)13\textsuperscript{18} already stressed that “the establishment of specialised units for the investigation of offences, the combating of which requires special expertise in information technology, should be considered.”

The answers to this question in the reports tend to highlight, on the one hand, the institutions that are responsible in general for the digitalization of the procedure, the automation of the justice system and the technical equipment of courts, which usually lies within the Ministry of Justice (for example, Austria, Brazil, Belgium, Croatia, Turkey, Spain); and on the other hand, the specialized units within the law enforcement agencies that deal with cybercrime, computer forensics, and internet surveillance.

All countries report to have special units to deal with cybercrime and with computer systems when fighting criminality. These “cyber-force” or high technological units are placed most often in the police structures, intelligence units of the law enforcement agencies and also in the public prosecution office (Argentina, China,

\textsuperscript{14} See CoE Rec (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes; and the CoE Convention on cybercrime of 23. XI. 2001 (hereinafter Budapest Convention).

\textsuperscript{15} See the Dutch report, under “An overview instead of a definition”, p.4.


\textsuperscript{18} Rec. No. R(95) 13, of the Committee of Ministers to Members States concerning problems of Criminal Procedural Law Connected with the Information Technology, adopted on 11.9.1995.
The European Union has since long seen the development and use of ICTs in the criminal field as a priority and this is evidenced, for example, by the Schengen Information System (SIS), a database set up for criminal proceedings. The personal data, which may include names, physical characteristics, place of birth, nationality, weather dangerous or not, etc., can only be used for the purpose of the alerts the data where entered. This information system is complemented with the network SIENA (Secure Information Exchange Network Application), mainly used by the EU member states to exchange information under the Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement agencies (for example, Belgium, the Federal Computer Crime Unit, Japan, Netherlands, Spain, Turkey, or USA). The USA report informs of the existence in that country of task forces—at least for law enforcement—involving in the implementation of the ICT in the criminal justice system: the internet Crime Complaint Center, a clearing house for the investigation of internet crime; the Cyber Initiative and Resource Fusion Unit analysing internet crime trends, but also filtering false leads before the information on cybercrime gets to the prosecution service (interesting within this unit is the support it gets from different private companies, as Microsoft or eBay, for instance); the U.S. Computer Emergency Readiness Team, which carries out no investigations, but gives support, coordinates and undertakes research projects; and finally InfraGard, part of the Department of Home Security, in which private and public actors share information, promoting dialogue between the ICT community and the law enforcement authorities.

Thus, at the level of criminal investigation, all countries studied here report to have responded to the needs of computer related crime and investigation by creating special units. It is not surprising that the special units for investigating cybercrime are also in charge of giving support to other units in the use of ICTs and forensic evaluation of electronic evidence in some countries (e.g., in Austria, Croatia, Spain). If these units are well equipped and have sufficient human and technical resources is a question not covered by this study. The UNODC report shows that the level of specialization is quite diverse, and that in many developing countries the level of training and capacities of those ICTs and cybercrime specialised units still need to be improved. However, attending to the development of the legal framework, as well as the literature and the information published in the media, it is evident that the USA has an intensive practice in using ICTs not only at the criminal investigation field, but also within the prevention of terrorism and national state security.

The answers within this study differ from other studies that cover also African countries, which state that African countries show a general lack of sufficiently specialized units, having some countries only specialized personnel within the general police departments. The European Union has since long seen the development and use of the ICTs in the criminal field as a priority and this is evidenced, for example, by the Schengen Information System (SIS), a database set up for criminal proceedings. The personal data, which may include names, physical characteristics, place of birth, nationality, weather dangerous or not, etc., can only be used for the purpose of the alerts the data where entered. This information system is complemented with the network SIENA (Secure Information Exchange Network Application), mainly used by the EU member states to exchange information under the Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the member states. The EU agencies set up for the cooperation in criminal matters at the police and the judicial level are Europol and Eurojust. Europol is the European law enforcement agency focused mainly on information exchange and intelligence analysis on cross-border serious crimes. It provides analytical support to the authorities of the member states and assists them in their criminal investigations. As de Busser states in her special report, “the Europol Information System (EIS) is, together with the Analysis Work Files and SIENA, the most significant tool when it comes to information exchange by Europol”.

\[19\] UNODC Comprehensive Study on Cybercrime, pp. 152-156.
\[20\] UNODC Comprehensive Study on Cybercrime, pp. 152-153.
\[21\] For the use of ICT and the data protection mechanisms at the EU level, we refer to the comprehensive special reports of E. De Busser and D. Brodowski, “European Initiatives Concerning the Use of IT in Criminal Procedure and Data Protection” which give answer to the whole questionnaire with regard to the European Union. Therefore the references to the use of ICT in the EU in this comparative general report will be kept to a minimum, referring generally to those two comprehensive and detailed reports.
\[22\] O.J.L 386, 29 December 2006
\[23\] For more details on the functioning of these tools and networks, see the report of E. De Busser, p. 12, and the literature cited there.
Eurojust is the EU institution for judicial cooperation and for supporting the cross-border criminal investigations of the member states; it has a case management system in place, which runs on the Commission’s secured s-TESTA network. At the EU level it is also worth mentioning the European Judicial Network24, providing for secure communications for judicial authorities; the European e-justice portal, where digitalised documents, relevant also for the criminal justice system (for example, legislation, competent authorities, etc.), are to be found25; and the ECRIS (European Criminal Records System), a decentralized system that provides a communication structure for requests on criminal records through standardized forms26.

The establishment of special centres for research and training in ICTs appears to be highly useful. The Belgian report mentions the “Cybercrime Centre of Excellence” for training, education and research in the public sector, where Universities, ICTs private companies, police, prosecution and judiciary work together.

Finally, it appears that specialization has been achieved at the police and investigation level, while the judiciary seems to remain largely non-specialised27.

(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?

Among the services that ICT providers offer to the criminal justice system we must distinguish between, on the one hand, technical and computer equipment (hardware and software) for the management of the administrative and procedural workload of the courts; and, on the other hand, the expertise or evidence provided at the different stages of the proceedings regarding the collection, manipulation and assessment of electronic evidence.

With regard to the first aspect, most countries do not have specific rules for computer equipment for administration of justice, but the general rules on procurement of the public administration apply. There is usually a public unit in charge of the automation of the management and the proceedings and such unit hires a private company after a public tender offer (for example, Belgium, Spain, Italy).

With regard to the second kind of possible cooperation in the different stages of the proceedings, the type of relationships between the private companies that offer ICT related services and the authorities of the CJS are reported to be very different. In some countries there is no legal provision on the hiring of private companies to provide services or forensics for the police, the prosecutors or the judicial authorities (Argentina, Brazil, Colombia, Finland); this may mean that they are not foreseen but are not excluded. Spain relies mainly on the expertise provided by the specialised public forensic units, often part of the police structure, but expertise can also be provided by private experts hired by the parties to the criminal procedure. In Austria, private companies will act only as experts. The judicial expert in Belgium is appointed by the judge in use of his/her discretionary power, and it can be a private person or company. In some other countries, despite the lack of regulation, there are single cooperation agreements between private companies and the actors of the CJS (Japan, Netherlands). Croatia’s report explains that there are companies that provide computer forensics, help in data recovery, and provide IT security. Many large consultancy companies have a department on forensics that provides expert ICT services in electronic evidence, mainly for the defence.

The EU relies in its own service providers and experts, and avoids to enter into agreements with private service providers. Interaction with private service providers may happen by way of expert reports on the integrity of electronic evidence.

In sum, it appears that, with regard to expertise or ICT forensics, two models of cooperation between ICT-related private companies and the CJS are the most common ones: one relies largely on private companies for the ICT criminal investigation, hiring forensic experts from private companies or among private persons; and a second model relies mainly on the ICT expertise provided by public entities or agencies, with only a minor involvement of private companies or persons in offering ICT support or expertise. Furthermore, all systems have mechanisms to compel private companies to cooperate within the criminal investigation.

As to other forms of cooperation, the EU Data Retention Directive of 200628 establishes an obligation for private telecommunications companies and internet providers to cooperate in the retention of data and the

---

25 See further the report of D. Brodowski, pp. 7-8.
26 See E. De Busser, p. 17.
27 Confirming this assessment also UNODC Comprehensive Study on Cybercrime, pp. 172-177.
surveillance of communications, subject to the legal requirements on the right to data protection and the right to privacy.

All the countries analysed have rules that impose on private service providers to cooperate in the criminal investigation, with different obligations regarding the data they are bound to store. Besides legal formal cooperation, there are also different degrees and channels of informal cooperation, which can be very effective for crime prevention and investigation but may pose severe risks for legal certainty, the rule of law and the protection of citizens’ fundamental right to privacy.

All of the reporting countries affirm that internet service providers and telecom companies are required to cooperate in providing data necessary for data protection, although not always for the hiring of experts. The limitations on the cooperation of private experts are subject to various limits: legal, financial and practical. In general, the rules on public procurement apply, although not always for the hiring of experts. The limitations on the cooperation of private experts are not clearly set out in the national reports, but generally there is legal duty to provide the expertise if required by a judicial authority, and the expert is obliged to confidentiality. As to the services supplied by service provider companies, it appears that the obligation to cooperate is subject to a judicial request and, in its absence, companies’ cooperation is restricted by the rules on data protection.

Cooperation with private entities or companies is subject to various limits: legal, financial and practical. In general, the rules on public procurement apply, although not always for the hiring of experts. The limitations on the cooperation of private experts are not clearly set out in the national reports, but generally there is legal duty to provide the expertise if required by a judicial authority, and the expert is obliged to confidentiality. As to the services supplied by service provider companies, it appears that the obligation to cooperate is subject to a judicial request and, in its absence, companies’ cooperation is restricted by the rules on data protection.

Some reports indicate that there are also cooperation agreements to share general information on ICT crimes, new technologies, types of searches, effective devices, carrying out software research, etc. As mentioned above, in section (1)(2), institutes or associations where experts from the telecom industry meet and exchange knowledge, discuss practical measures, and share information on technical issues—as well as risks and threats—with scholars and law enforcement authorities, are in place in several countries (Belgium or the United States, for example), and appear to produce good results for each of the parties involved.

2. Information and Intelligence: building information positions for law enforcement

Building up information positions is part of the so-called intelligence-led-policing (ILP). Intelligence-led-policing 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, particularly state security issues, and fight against most serious forms of crime, as terrorism and severe phenomena of transnational organized crime (TOC). The information is gathered and analyzed with the aim of designing and establishing a certain police strategy (management or criminal policy), a tactic approach, an action plan, or a concrete operation (missions, controls, inquiries). Within the EU, the intelligence-led policy was emphasized in the Hague Programme of 2005 with the aim of improving the efficiency in the fight against organized crime.

An “information position” or “Big data” is the result of bringing together a large mass of data stored in different data bases and processing these data for specific purposes. This term may be considered equivalent to

29 “Article 4: Access to data.— Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.”
30 In the same sense also UNODC Comprehensive Study on Cybercrime, p. 151.
33 See E. De Busser p. 8.
intelligence, although the term “intelligence” has different meanings. One of these meanings, following the 
Analytical Guidlines of Europol, prepared in 2000, is “processed information”, i.e., the product of the development of the circle of intelligence, which implies the collection, selection and evaluation of the information34. A similar definition is given in the Law Enforcement Analytical Standards made by the US Department of Justice35, which, however, makes a distinction between “intelligence” and “tactical intelligence”. In accordance to these definitions it is not easy to differentiate the meaning of “building information positions” and “intelligence activity”, as both refer to the gathering and processing of data. Nevertheless, the concept of “intelligence” is traditionally associated with secret services and state security. This might explain why in the European area some countries have opted for using the term “building information positions”, to make clear the distinction between the activities of intelligence for state security purposes, subject to broader powers and usually not so strict controls, and the information the law enforcement authorities gather to be better prepared to fight against crime at the preventive level—or at least not connected to a specific crime that has been committed—in which generally it is not allowed to resort to coercive measures. In the Resolution regarding “Special Procedural Measures and the Protection of Human Rights”, adopted in the XVIIIth International Congress of Penal Law held in Istanbul in September 2009, it was already stated that: “The collection of digital information for law enforcement purposes should be regulated by criminal procedure”36. These conceptual differentiations are not always clear, either at the legal level or in the scientific literature. Therefore it is understandable that many national reports have answered the questions related to “building information positions” by referring also to the activities of the state security intelligence units.

The conceptual changes in substantive criminal law37 have caused the transformation of the criminal procedure, which was traditionally conceived as a reactive response, to become a pro-active mechanism, and as a consequence the dividing line between intelligence authorities and law enforcement authorities is becoming blurred38. As the notions of prevention and repression of crime tend to disappear, or at least are not completely separated anymore, pro-active investigation techniques are applied to gather and analyse information on the trends and risks of criminality as well as about criminal structures and preparatory acts. The long-established principle of separation between secret intelligence functions and law enforcement criminal investigation (Trennungsgebot) is increasingly changing towards a cooperation model, where intelligence units deal with criminal investigation and law enforcement authorities elaborate intelligence39. The fight against complex forms of transnational crime has led to the use of massive amounts of data, which require not only special software to carry out the data mining, but also a selective and

35 Intelligence: Information + Evaluation. The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities. Intelligence is information analysed to determine its meaning and relevance. Information is compiled, analysed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. Tactical Intelligence: Information regarding a specific criminal event of immediate use by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. Available at: http://www.ialeia.org/files/docs/law%20enforcement%20analytic%20standards.pdf
36 This point 14 continues: “In the case of privacy-related information, a court warrant is required, The threshold for compelling data from service providers should be higher than the “relevant for the investigation” standard”. See XVIIIth International Congress of Penal Law (Istanbul, Turkey, September 2009), Istanbul 2009, p. 172.
38 See the very illustrative conclusions of J. VERVAELE, “Special procedural measures and the protection of human rights”, General Report for the XVIIIth International Congress of Penal Law, Istanbul 2009, pp.138 ff., which do not only underline the changes in criminal procedure and intelligence activities, but contains a very interesting overview of this transformation from a comparative point of view. See also L. Bachmaier, Información de Inteligencia y proceso penal, in T errorismo, proceso penal y derechos fundamentales, pp.56 ff., and the literature cited there.
39 See, for Germany, for example, A. ABBÜHL, Der Aufgabenwandel des Bundeskriminalamtes, Stuttgart 2010, pp. 353 ff.
professional analysis of such data to identify targets and risks relevant for the security and for the criminal justice system.

(1) Which ICT-related techniques are used for building information positions for law enforcement agencies?

Before analysing the answers to this question, it must be noted that most national reports do not distinguish between information gathered for criminal policing and strategies, on the one hand, and information related to state security and/or crimes capable of affecting the state security (terrorism, organised crime), on the other hand. To some extent this is not surprising, as the concept of “building information positions” is still unknown in many legal systems, and only recently the activity of the police and other law enforcement agencies in the preventive field (or carrying out exploratory investigations, as it is written in the Dutch report) has attracted the attention of legal scholars. Since the borderline between prevention and repression of crimes tends to be increasingly blurred in many areas, the gathering of information not linked to a certain crime already committed, but directed to identify the risks in the criminal field, becomes more and more relevant. However, traditionally the CPCs do not regulate these activities, as they are considered to be outside of the criminal procedure. On the other hand, many police laws do not regulate the powers and conditions to carry out measures whose aim is to identify risks and set up preventive strategies, because traditionally the protection of privacy generally was only taken into account within criminal investigation, and not within intelligence led activities.

It appears that for preventive objectives, strategic planning, and state security objectives, the conclusion to be drawn from the reports is that in most countries all kind of ICTs are used for surveillance and monitoring of communications, to trace financial data, geo-location devices, automatic license plate recognition, secret acoustic and video surveillance, processing of images, data-mining and matching, wire tapping and network interceptions, thermal imaging technology, beepers, or other tracking devices. The Chinese report refers generally to “other secret means”, while the US report lists, in a very detailed way, all kind of techniques and devices to undertake extensive surveillance of communications and movements and access to different data bases; it even mentions the use of drones—often utilized to monitor movement on the US borders—for policing. The use of drones has caused wide controversy, moving the Federal Congress to pass a bill on February 2013 prohibiting their usage for targeted surveillance of individuals or property without a judicial authorization.

It seems that within intelligence activities—it is not clear if broadly or strictly conceived—states resort to all possible kinds of available technical means, depending on their financial resources or their assessment of security risks. The practices followed by each country with respect to these devices are not known and fall out of the scope of this study. The conditions and requirements to utilize those ICT-techniques are unclear, for generally the reports’ answers to the questionnaire do not distinguish between intelligence services in the realm of state security and building up information positions by law enforcement agencies.

The USA system has a broad regulation on government powers to conduct national security surveillance, but the dividing line between criminal investigation and national security—as occurs also in other systems—is not perfectly defined, being unclear when the data obtained under a security surveillance may be used as evidence in a criminal procedure. The Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) have collaborated since the 1940s in secret domestic intelligence operations. The Foreign Intelligence Surveillance Act (FISA) of 1978, amended several time since then, regulates the surveillance of foreign agents, foreign citizens or foreign threats, and establishes different requirements and safeguards depending on whether the surveyed person is a US citizen or a foreign citizen—lower standards of protection are applied in the latter case.

It is worth to have a closer look to the Belgian report, because it is one of the few reports that draw a clearer distinction between building information positions and secret services intelligence activities. As explained in this report, there are mainly three different techniques related to ICTs that can be used for building up information positions: access to databases, surveillance systems, and statistics. Access to databases and

40 See USA report, p.22: “for the purposes of the application of the Foreign Intelligence Surveillance Act a foreign power includes not only a foreign government or an entity under the control of a foreign government, or a foreign-based political organisation, but also a group engaged in international terrorism or activities in preparation therefor, and an entity not substantially composed of US citizens or residents that is engaged in the proliferation of weapons of mass destruction”.
processing of data are specifically examined in the next subsection. Therefore, we will focus here on surveillance activities and statistics.

For building information positions two types of electronic surveillance systems are allowed in Belgium: the video-surveillance in public spaces and the use of satellite images. Video surveillance by fixed cameras in public spaces has to be explicitly indicated in the relevant places and cannot be directed to obtained intimate images. If the images are relevant from the criminal perspective, the police shall inform to the judicial authorities. Mobile cameras are allowed, if authorized by the municipality, for special public events and are limited to the time of those events, to prevent and detect possible alterations of the public order, concrete dangers for the security. In case of commission of a criminal offence, the police may request the recorded images. The use of the so-called “intelligent cameras” is still controversial: there is no precise regulation of its usage and the legal provisions for standard video-cameras are applied, although this might infringe the right to privacy by providing information related to the political, religious, ethnical or sexual information of the person under surveillance by an “intelligent camera”, as it may trace all the movements of a person or a vehicle.

Finally, the processing of statistical information is mentioned as one of the sources of information for building up information positions but is considered to need improvement, because the lack of sufficient statistical data does not allow an accurate analysis.

At this point it is clear that it is necessary to agree on which powers the law enforcement agencies should have in their role of building information positions, as the use of ICTs opens so many possibilities to obtain and process data that it endangers the privacy of citizens. This is not an easy issue, for it requires defining also the notions of security or prevention functions as well as the notion of strictly criminal investigative acts. As long as both spheres—preventive and repressive—are not strictly separated, the powers of the law enforcement agencies in building information positions are also difficult to define.

(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?

Some reports answer this question by stating that all kind of data bases can be accessed by law enforcement agents if there is a prior judicial warrant (for example, Brazil, Colombia), and hence it is unclear which data-bases can be accessed in those countries directly by law enforcement agencies. Other countries report that public databases can be accessed directly but, if sensitive personal data are concerned, a judicial warrant is then required (Italy, Netherlands). Photographs are considered, according to the data protection law, as “sensitive data” in The Netherlands, as they allow identifying ethnic origins and/or religious beliefs of the person. In general, it seems that all countries allow law enforcement agents to access open-source public or private databases, databases of fingerprints, ID registers, car registers, information systems like Europol or Interpol, data on the register of hotel guests, customs, arms register and criminal police file index; in such cases, law enforcement agents can access directly those databases or records, without prior judicial warrant, but access may be subject to certain controls, passwords or internal authorisation, only within the job description). Within the European Union, member states’ law enforcement authorities can also access the Visa Information System (VIS), which contains biographic and biometric data of persons that have applied for a visa in the Schengen area. To be granted access to this database, the relevant law enforcement authority must show that such access is necessary for preventing, detecting or investigating terrorist offences or other serious criminal offences41. Under similar conditions, and also for the prevention and detection of terrorist or other serious offences, law enforcement authorities and Europol are provided access to the EURODAC database, which contains the data of persons that have lodged an application for asylum in any of the EU member states. Due to the action of the European Data Protection Supervisor (EDPS) which has expressed concerns regarding the right to data protection, since 2013 access to this database is verified by an independent authority in each members state42.

In general, if we take into account only the information contained in the national reports, it is unclear if direct access to databases is only permitted within a criminal investigation or if it is also allowed for building information purposes. In the USA, however, it is unmistakably defined which data can be accessed without infringing 4th Amendment: law enforcement agents can have access, without any additional requirement, to the so-called “envelope data” and “metadata”, websites visited, telephone numbers dialled, and subscriber

41 See E. De Busser, p.17.
42 See E. De Busser, p.18-19.
information, because it is considered that there is no reasonable expectation of privacy for those data. The Customs Information System (CIS) contains a file identification database with biographical data and business data, which can be also accessed by law enforcement authorities of the member states, Europol and Eurojust.

If we focus on DNA data bases, the answers show a quite different picture: while in USA or Italy a judicial warrant is needed, in Austria, Belgium, China (State Bureau Agency), Croatia, Japan, and Spain it seems that DNA data bases can be accessed without judicial warrant. However, from the scope of the answers it is not clear if the police that can access the DNA data bases, has also the powers to order the matching of DNA profiles. Turkey reports that they do not have DNA databases.

With regard to the access to private databases, they are only accessible within a criminal investigation, but not for preventive purposes (Austria, Belgium, Brazil, Colombia, Finland, Japan, Netherlands, Spain) and generally only after obtaining a judicial warrant, except for those databases which are open-source (Sweden).

(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?

Sophisticated programmes have made it possible to mine a huge number of data from the intelligence community and internet searches and, as has occurred in the USA, a mixture of commercial and public sector resources, known as “fusion centres”, have optimized the collection, analysis, and sharing of information regarding data about banking and finance, real estate, education, retail sales, social services, transportation, postal and shipping, lodging transactions etc. All this information can be made accessible with no more that a name, address, phone number or social security number. These data mining tools allow acquiring in very little time a huge amount of information regarding a group or “persons of interest”, making profiles of possible suspects or groups of risk. Data mining can be “target-driven”, which involves obtaining information about an identified suspect; “match-driven”, to see whether a particular person is a “person of interest”; or “event-driven”, to discover the perpetrator of a past event. Undoubtedly the targeted processing and analysis of such a broad array of sources of information, even if they are open-source information, may represent an intrusive measure in the privacy of a citizen. Nevertheless, most legal systems lack clear regulation on data-mining, as well as to the cases and circumstances in which it can be applied, by whom, what are the conditions to undertake such collection and processing of information, and if the data mining can be also used in the preventive field for the profiling of potential perpetrators. While there is lack of adequate regulation (for example, Argentina, Brazil, Belgium, Colombia, Spain; and also Italy, which regulates only the DNA data bases). It appears to be widely used in practice in most countries, at least in the preventive field and by intelligence services (the only report that clearly states that data-mining techniques are not used/allowed is Argentina).

This poses a significant problem, as it means that data mining and data matching are being applied without a clear legal basis. Usually, if the accessed data are open-source, it is considered to be open to every one that have access to internet, and thus the privacy protection should not apply—it would be similar to a surveillance operation on the street carried out by agents. And if the data are not open-source, then these cases are to be handled on the same legal basis applicable to communications interceptions. However, this does not provide a sufficiently foreseeable legal basis to grant adequate protection to the privacy of citizens, and the majority of people are unaware of how far their data on the web can be mined and analysed within seconds, and therefore their movements, activities, and transactions can be traced and identified accordingly. Lacking a specific legal basis, it is unclear if the data mining requires some previous probable cause or suspicion, or if it can be carried out for profiling groups and potential perpetrators.

The countries that have specific legal provisions regarding data mining present a wide spectrum as to the requirements for its lawful use. Austria allows data mining upon simple suspicion of a crime with a custodial

43 As for example, ADVISE (for Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), Verity K2 Enterprise (a programme of the US Defence Department for identifying foreign terrorists and American citizens connected to foreign intelligence activities), TALON (Threat and Local Observation Notice), STAR (System-to-Assess-Risk), “XKeyscore” (which filters out information in clear text and registers metadata as well as content data if it conforms to specific buzz words), or CARNIVORE (a programme for interception and duplication of e-mails at time), as cited in the USA report, pp. 57-61.

44 USA national report p. 60.

45 We follow here the definition contained in the USA report, p. 1.
Undoubtedly, the largest development of data mining programmes is to be found in big countries with a relevant role in global security and with important economic interests worldwide. These countries spend huge amounts of money in security programmes and in the fight against terrorism. The USA appear to have and relevant role in global security and with important economic interests worldwide. These countries spend huge amounts of money in security programmes and in the fight against terrorism. The USA appear to have a undisputed leading position in the collecting and processing information with data mining programs— or amounts of money in security programmes and in the fight against terrorism. The USA appear to have and relevant role in global security and with important economic interests worldwide. These countries spend huge amounts of money in security programmes and in the fight against terrorism. The USA appear to have a

undisputed leading position in the collecting and processing information with data mining programs, –or perhaps this apparent leading position is due to the fact that the extensive use of data mining in this country has been made public, while other countries may also be using them but no information has leaked to the media–. The USA system regulates the collection and analysis of foreign intelligence by the NSA, which, as already mentioned, is directed to the surveillance of “foreign powers”; and also the collection and analysis of foreign data mining, combining and analysing. The analyses are classified attending to their authenticity and reliability (confirmed and non-confirmed information).

46 See E. De Busser, pp. 34-35.

What is crucial to the criminal procedure is not only the possibility to undertake surveillance and interceptions within the proactive stage, but also to check if the findings and information so collected can be used later as evidence or not. Even if these intrusions are very grave from the perspective of the protection of the right to

penalty of more than 10 years. If sensitive data like ethnic origins, political opinions, religious believes or sexual life are included, then a judicial warrant is needed. In principle, no data mining is permitted out of these cases, due to the Data Protection Law. In Belgium data mining is utilized within the tax administration to detect tax frauds, but no other profiling is foreseen by the law. Japan, Turkey and The Netherlands apply data mining, but in principle not for creation of profiles of possible perpetrators or risk groups, while in Sweden the profiling of persons or groups is also admitted. It appears that data mining may be used for preventive as well as for criminal investigation purposes, but it is unclear under which conditions and with which limitations.

At the European level, the data provided by the law enforcement authorities of member states are used for data mining, combining and analysing. The analyses are classified attending to their authenticity and reliability (confirmed and non-confirmed information).

(4) Can coercive measures (e.g. interception of telecommunications) be used for building up information positions?

Although the question was directed to know about the use of coercive measures within the proactive stage of the criminal investigation or the building of information positions, the answers are focused on the use of telephone tapping. In this regard, we face many variegated answers. Some countries exclude the possibility of using wire tapping at this stage (Belgium, Sweden), while others adopt the opposite solution, which allows them very broad powers for intelligence led policing (Finland and China). Most countries either condition the use of coercive measures in the preventive stage to obtaining a prior judicial warrant—even if such authorization may be only a formality, as the grounds for issuing it will not be checked (Argentina, Brazil, Japan, Italy, Spain or USA, for example)— or limit their use to certain types of crimes, such as organized criminality or cybercrime (e.g., Austria and Croatia). However, no definitive conclusions can be drawn from the national reports, for some of them do not differentiate clearly between the domain of secret intelligence service activities (state security) and intelligence led policing measures for the building of information positions by law enforcement agencies. This is especially the case of the USA, where the concept of "building information positions" is unknown. Therefore, the information provided in the USA report deals with the activity of state security intelligence activities, be it at the domestic level or directed to the surveillance of foreign powers. Within the intelligence activity, either carried out by the CIA or by the NSA, interception of communications and access to stored mails can be ordered. These coercive measures require a judicial warrant if they are targeted to a US citizen, but otherwise not. In the case of FISA activities, the gathering of information through wiretaps or search of electronic communications is subject to judicial control, and falls within the competence of the Foreign Intelligence Surveillance Court.

What is crucial to the criminal procedure is not only the possibility to undertake surveillance and interceptions within a proactive stage, but also to check if the findings and information so collected can be used later as evidence or not. Even if these intrusions are very grave from the perspective of the protection of the right to
privacy, their utilization in a criminal procedure should not be necessarily criticized, as long as the exclusionary rules apply. Italy traces a clear line: the interception of communications ordered by the PP for preventive aims have no evidentiary value. The problem is—as the Turkish report remarks—that the exclusionary rules are not always respected, and those proactive interceptions, ordered without probable cause or even without judicial warrant, may end up as evidence at court.

(5) Which private actors (e.g., internet providers or telecom companies) retain or are obliged to retain information for law enforcement agencies?

All telephone companies, and later internet service providers, registered the telephone calls of their customers, the origin and the recipient of those communications, and their duration for billing purposes. Once the billing process was ended, those data were generally deleted. However, all that information about traffic data and internet connections have been considered essential for the investigation of severe crimes, especially for terrorist attacks. For this reason, a number of countries considered the convenience of establishing a legal obligation to retain and store those data for a minimum time, in case such data might be necessary to investigate and prosecute serious crimes. This explains why the EU adopted the much-discussed Directive on Data Retention. The Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network (art. 1.2). The Directive establishes: the obligation to retain data for a period of time not inferior to 6 months (art. 6); which data must be retained by the companies (arts. 3 and 5); the conditions to make them available (arts. 4 and 8); and the requirement that data protection rights must be respected (art. 7). Therefore, it can be stated that within the EU there is a harmonised legal framework with regard to the obligation to retain data by private companies that provide telecommunication services.

In the USA, the Electronic Communications Privacy Act 18 U.S.C. §§ 2701-2711, provides also for a data retention obligation. As to other non-EU countries studied, generally the reports state that there is an obligation for the telecom and internet service providers to retain and store communications data upon judicial request (Argentina, Brazil, Colombia, Turkey). However, as occurs with respect to other questions, it is unclear if the obligation to retain data upon a judicial warrant needs to have connection with a criminal action or can be ordered with a preventive purpose. It appears that there is such an obligation in Turkey (for a period between 6 months and 2 years), but out of Europe service providers frequently do not have the obligation to retain communications or computer data.

(6) Which private actors can provide or are obliged to provide information to law enforcement agencies?

When asking about cooperation between private actors and law enforcement authorities with regard to the use of ICTs, the answers tend to focus on the cooperation with telecommunications companies and internet service providers. This is logical, as the cooperation of these type of companies is essential in the prevention and investigation of serious crimes. But there might be other types of companies involved which cooperate in investigating and preventing crimes and also use ICTs, e.g., video surveillance. In this paragraph, we will deal mainly with those data that provide communications services and store computer data.

The importance of their cooperation has been recognized in the Cybercrime Convention of 2001, whose art. 18.1 provides that national criminal procedures must establish measures to require companies and citizens to hand out subscriber information or other specified data. Such cooperation is relevant for prosecuting not only cybercrime but also all crimes where the use of ICTs is allowed and necessary. The key question is how far and under which conditions should these companies be obliged to provide the information requested by law enforcement agencies. The answers to this question should focus on the information they are obliged to provide.

---

47 This Directive is currently under review. The Commission's evaluation report made in Brussels, 18.4.2011 (COM(2011) 225 final), concluded that the EU should continue to support and regulate the storage of, access to and use of telecommunications data. However, EU rules in this area need to be improved to prevent the different types of operators from facing unfair obstacles in the Internal Market and to ensure that high levels of respect for privacy and the protection of personal data are applied consistently. The EU has set up a working group to review this legal instrument. An interesting study on the impact of the Directive is reflected in the independent study “Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries” of November 2012, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf.

48 See UNODC Comprehensive Study on Cybercrime, p. 145.
provide within their functions of building information positions and not within a criminal investigation. However, here again the field of proactive investigation and crime investigation/prosecution does not seem to be clearly separated.

All countries report that private actors are obliged to supply information to the police upon a judicial order, and in some countries (Italy, Netherlands) also upon the request of the public prosecutor. This could be interpreted in the sense that there is no obligation to provide any information to the police but only to the judicial authorities or, exceptionally, to the public prosecutor. However, this would not be a correct conclusion because, as the questionnaire does not distinguish between the different types of data, the national reports have not always addressed the distinction between metadata and content data. However, if this question is interpreted in connection with the previous one, it might be understood that the content data may not be obtained without a judicial warrant and usually only within a criminal investigation. As far as the other data are concerned, the report on Croatia clearly states that the police can obtain from the service provider companies all non-content data (identity, traffic data, geo-location) for preventive aims, with the authorization of the Head of the Criminal Police. In Spain the IP number can be obtained without judicial warrant: although there is no legal provision on this issue, according to the Spanish Supreme Court, as long as the IP does not allow to identify a certain person, it does not affect the right to data protection, and thus no judicial order is requested. Only one country (Japan) states that there is no obligation to cooperate with the police in building up information positions.

The situation in the USA deserves a special analysis, not only because of the existing extensive practice of cooperation of private internet service providers with law enforcement agencies, but also because of the numerous rules that regulate cooperation between police in general and telecom companies. Under the FISA and the Communications Assistance for Law Enforcement Act (CALEA), companies have the obligation to provide not only data to the police, but also information, facilities and/or technical assistance necessary to intercept wire, oral or electronic communications, or to conduct electronic surveillance. Non-compliance with those legitimate requests can lead to obtaining a court order. In case of infringing the court order, the company can be fined. Service providers cannot disclose the existence of any interception or surveillance upon penalty of civil damages. Furthermore, the law states that they are not liable towards their clients for cooperating with the law enforcement agencies following statutory authorization or for complying with the court order. As the USA report indicates, only AT&T responds to an average of more than 700 requests a day, of which 230 are regarded as emergencies and thus do not require a judicial warrant.

The practice has also shown that there has been a special relationship between some companies (precisely AT&T and NSA, by which the intelligence agency was allowed to access directly all content data. A special program allowed also access to the data of Microsoft, Google or AOL, for the purposes of data mining. It has been recently published that NSA had control over the fiberglass cables, which allowed the secret intelligence agency to access directly to all data, without entering agreements with the private companies.

With regard to the cooperation of private service providers with foreign authorities, usually the companies will only provide data requested upon a judicial warrant or order issued in the “seat” jurisdiction of the service provider. However, Google, for example, reports that they have sometimes cooperated with foreign authorities on a voluntary basis if the request was consistent with international norms.

The Netherlands’ report mentions another type of cooperation between law enforcement authorities and private companies: the specific observation of persons or places carried out by a private security company (Securitas). Law enforcement authorities provide the company with pictures of persons, places or cars that should be observed; and the security company gives the police all the images they have taken or the videotapes resulting from their surveillance.

(7) Is there judicial control on building information positions?

The approach varies from country to country. In the majority of countries it appears that the building of information positions, if this activity is legally regulated, is not subject to judicial control (Belgium, Croatia, Italy, Netherlands, Spain), except when measures restrictive of fundamental rights are taken (Colombia or Croatia) or when extremely sensitive privacy data are affected (Netherlands). In Austria, although police activities based on security or intelligence-led objectives are not subject to the control of the judiciary, such control is exercised by a legal independent attorney located within the Ministry of Interior. This attorney

49 See UNODC Comprehensive Study on Cybercrime, p. 150.
performs three types of supervision: in advance, by granting the authorisation; ex-post, by providing information and comments on the measures taken; and finally, by notifying the relevant authorities about the activities carried out. Belgium does not have a judicial control over police activities related to building information positions, but has a Parliamentary Commission to protect the right to privacy and the right to data protection. The system works upon the reception of claims; after study, a mediation and conciliation is sought, and if not achieved, a recommendation and warning is issued. This Commission can also receive complaints regarding infringements of the right to data protection by police authorities. This would represent an indirect control of the activities of the police in building up information positions, but with the limits of being a system of control ex post, and with a limited scope.

3. ICT in the criminal investigation

(1) Can law enforcement agencies carry out interception in real time of a) e-traffic data; b) content data?

Relevant electronic evidence may never be stored and thus require a real time interception in cases of urgency and due to the volatile character of electronic data. Many international and regional conventions and instruments on cybercrime include provisions in real time collection of computer data51. All the reporting countries, except Japan, indicate that the interception of electronic communications in real time can be carried out in their legal systems, either by applying the general rules on telephone tapping or interception of communications (e.g. Argentina, Italy, Spain, or Turkey) or by applying special rules on interception or search of electronic communications. The extended practice of using telephone tapping rules as a legal basis for interceptions of electronic communications is not free from problems52. For example, in Turkey, the rule on the interception of telephone communications uses the verb “listening”, which is not suitable for the interception of images and messages, thus raising the question about whether it could serve as a legal basis for e-traffic and content data real time interceptions. In practice, the Turkish courts have accepted a broad interpretation of the term “listening”, with the consequence that the rule for telephone tapping is applied to electronic interceptions if the same requirements are met.

Most countries —China is the exception— require a prior judicial warrant for this measure: Austria (arts. 134 and 135 CPC), Belgium (art. 88bis and 90 CPC) Brazil, Croatia (art. 332 CPC), Finland, Italy (art. 266 bis CPC), Netherlands, Spain (art. 579 CPC, except for meta-data, which can be obtained without judicial warrant), Sweden, Turkey (art. 135 CPC) and the USA (except for meta-data, for which, depending on the states, the judicial warrant may not be required). The US law, however, makes a distinction between wire-tapping and electronic communications. For electronic communications, held in storage in a service provider for 180 days or less a search warrant showing probable cause is needed. But if the data are stored for more than 180 days, a subpoena or court order without showing probable cause will be sufficient, as far as it is shown that the data are relevant for a criminal investigation. These different requirements, as explained in the USA report, are due to the fact that Congress analogized the short-term storage of electronic contents to a safety-deposit box, and long-term storage to business records held by third parties. This unusual approach, not found in another country, gets even more complicated because the rule applies differently depending on whether the recipient has accessed the message within 180 days or not. It is interesting to note the statistical data on the practical application of these measures in the USA: a congressional inquiry determined that cell phone carriers responded in 2011 to 1.3 million demands from law enforcement agencies for text messages and other information about subscribers53.

Exceptionally, in cases of urgency, the interception of electronic communications can be ordered by the public prosecutor, subject to an a posteriori judicial control. Once the warrant is issued, some systems allow the direct access to the data using special software (for example, Brazil, Spain or USA), while others must request the cooperation of the relevant telecom or internet service provider company. The judicial warrant has to be motivated, and the measure must comply generally with the requirements of necessity, adequacy and proportionality, expressed by the ECtHR when interpreting art. 8 ECHR. Some countries limit the use of this measure—in similar terms to telephone tapping—to certain categories of crimes, which are either listed

51 For example, art. 20 of the CoE Convention on Cybercrime; art. 29 of the League of Arab States Convention or art.19 of the Commonwealth Model Law.

52 On this issue in Spain, see J.C. Ortiz Pradillo, “Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica”, in El proceso penal en la sociedad de la información (J.Pérez Gil ed.), Madrid 2012, pp.267-310, 300.

53 See USA report, p.28.
and preventing the deletion of computer data. However, many of the reports indicate that precise legal provisions for search, seizure and freezing of computer data are lacking, and therefore these measures are only carried out under the general rules of search and seizure of movable things (e.g., Argentina, Austria, Croatia, Belgium, Spain), or under production orders or document disclosure orders. These solutions may be acceptable as far as they are provisional, until the legal framework is updated, but they are not fully appropriate when dealing with computer and online data. The slowness of the law-making power to update the procedural rules is certainly striking, especially in the pan-European landscape, where the CoE Procedural Law Connected with the Information Technology, adopted in Strasbourg on 11 September 1995.

One exception in this respect is Belgium, where the interception of electronic traffic and of content data are regulated in different rules and subject to slightly diverse requisites. On the one hand, art. 80bis of the Code d’Instruction Criminelle (as amended in 1998) applies to all forms of telecommunications and regulates the recherche et localisation des telecommunications. This provision covers the interception of e-traffic data: IP-address, e-mail address used, websites visited, servers connected, log-ins on private sites (peer-to-peer, file sharing, etc.) and history of connections. Such measure requires as a rule a judicial motivated warrant, can only be adopted within a criminal investigation procedure (but not in the preventive setting by law enforcement authorities), is limited to a duration of 2 months (that can be extended), and is not limited to certain offences. To demonstrate the necessity of the measure, the investigating judge does not have to present evidence that other less intrusive measures have proved to be inefficient. On the other hand, art. 90 ter and quater of the Code d’Instruction Criminelle regulates the interception of content data of electronic communications in real time. The main differences between the access to e-traffic and content data are: the level of suspicion required (higher for content access), the duration (shorter for the content data), and the fact that access to content data is limited to serious offences and it allows to enter the home to install devices to facilitate the access to the content data. In practice, art. 90 ter and quater are more commonly used, as they allow access to a much broader information.

The Belgian report points out another interesting issue, related to the interceptions of electronic communications in real time. It assumes that this measure refers to the possibility of accessing those communications when they are being transmitted (en transmission). However, it is unclear when an electronic message is being transmitted or when it is already sent and would fall under the category of “stored data”. A part of the Belgian jurisprudence initially understood that the transmission of an electronic communication was not finished until the recipient accessed the message, while other judicial decisions considered that the transmission ends at the very moment that the message is in the webmail, and thus accessible to the recipient, regardless when it is actually read by him.

(2) Can law enforcement agencies have access to/freeze/search/seize information systems for a) e-traffic data; b) content data?

All reporting countries answer this question in the affirmative, in conformity with the most relevant international and regional cybercrime instruments, which require states to establish provisions for accessing and preventing the deletion of computer data. However, many of the reports indicate that precise legal provisions for search, seizure and freezing of computer data are lacking, and therefore these measures are only carried out under the general rules of search and seizure of movable things (e.g., Argentina, Austria, Croatia, Belgium, Spain), or under production orders or document disclosure orders. These solutions may be acceptable as far as they are provisional, until the legal framework is updated, but they are not fully appropriate when dealing with computer and online data. The slowness of the law-making power to update the procedural rules is certainly striking, especially in the pan-European landscape, where the CoE Recommendation R(95) 13, adopted on 11 September 1995, already emphasized the need “to adapt the legitimate tools which investigating authorities are afforded under criminal procedural laws to the specific nature of investigations in electronic information systems”.

---

54 Belgian report, p. 36.
55 See for example, art. 16 of the CoE Convention on Cybercrime of 2001. With regard to other covenants, see UNODC Comprehensive Study on Cybercrime, p.127.
In this context, with regard to access to data, there are several questions not clearly covered by the traditional provisions on search and seizure of movable things. If the objective of the search are the data stored in some hardware (hard-disk, CDrom, USB-pen drive, GSM or tablets, for example), then the rules for the classic search and seizure could be applied analogically, and generally they would suffice, but even if this is true, identifying which rules are exactly applicable might be problematic. In the case of a computer located in a private home, to access the stored data in the hard disk usually it will be necessary to enter the home and seize the computer equipment. The rules for home searches would apply and most countries—not all—consider that the warrant to search a home allows searching the data stored in a computer (disk, USB stick, etc.) that has been found in the place. However, if the data to be seized are stored in a computer located in a public space—for example, a cybercafé or a public library— are the rules for enter and search a public space applicable or, as the computer data should be considered private, should the rules on search of private dwelling be applied?

The scholars do not agree on this issue, and their position depends on their conception of the privacy. If they focus on the protection of the privacy of the data, then the location of the hardware in a private or public space would be irrelevant, for in any event the search of the computer would fall under the privacy protections of art. 8 ECHR. But, if the accent is on the place where the computer was connected, and that place was public, then the relevant computer data could be considered also publicly accessible or requiring only a search warrant for public spaces.

The issue turns out to be even more complex when it comes to the search of data that are in a computer system or are accessible through a computer network. In such cases, the rules of search and seizure of movable things are not always appropriate. First, the whole computer system cannot be moved to the police premises to be searched and analysed (for example, the whole computer system of a bank or a hospital), with the consequence that the computer system must be searched and registered on the spot, without moving the hardware, and it is necessary to provide for the seizure, securing or freezing of the computer data directly. Second, if the access to one computer allows the access to a network of computers that are on line, we have to face the question about to what extent the order to search a precise computer covers also the remote access to all other computers connected to the same network. The problems posed by this extended search (netwerkzoeking, in Dutch) are described in detail in the Belgian report. If the computer which is being searched in a home is connected to other computers located elsewhere, in principle, if the traditional rules on search of movable things should apply, an additional search warrant should be issued to access the data stored in the other computers located elsewhere. On the contrary, if the search of the computer is assimilated to a home search, in that case the consent of the owner or user of the computer to access it, would also serve for accessing the computer network—it would be comparable to allowing access to all the rooms of the house, although the extended computer network search could not go beyond the data accessible to the user whose computer is being searched. In other words, remote access to computers through hacking by the police—without consent or judicial warrant—should not be permitted, for this would amount to an illegal entry. The Dutch law specifically regulates this possibility, but has to be authorised by the Examining Judge upon elements of suspicion of a possible crime

The foregoing examples illustrate that there is need for a clear understanding of the meaning of “enter and search” of a computer, and there is also a clear need for developing the legal framework to elucidate the scope and requisites of these measures. In other words, a precise and clear legal statutory basis is lacking in all the reporting countries. Although the CoE Cybercrime Convention of 2001 already established that the Convention member states should adopt laws to ensure that the authorities can carry out extended searches (art. 19.2), several states seem not to have implemented this provision in their respective legal systems. The lack of specific regulation is also highlighted in the UNODC Comprehensive Study on Cybercrime: with regard to investigative powers, the main gap identified was the lack of legal mechanisms to enter computer networks in order to search for evidence, and to expeditiously preserve the computer data.

With regard to the seizure, securing and freezing of electronic or digital data, the problems are less complex, but it cannot be stated that there are no problems. Usually, if, through the ordinary search, computer search or network search data that are relevant for the criminal investigation have been found, those data can be seized. If the data are in the hard disk of the computer, in a USB stick, tablets, smartphone or CDrom, those elements can be seized according to the traditional rules of seizure of movable things. If the data are in a

57 See report of the Netherlands, p. 16.
58 See pp. 124 ff.
Within this context, several issues remain unclear. First, if general production orders are to be used to obtain and secure the data, these orders usually require identifying the object, the information or the documents to be disclosed. This is not always possible during the search of a computer network, where it might not be defined which is exactly the communication that is relevant for the criminal investigation. Moreover, preservation orders should be subject to the assessment of the proportionality of the measure, a requirement that is not easy to fulfill in short time, because of the huge amount of data that have to be first checked, until the preservation order is issued. Due to the risk that important data are deleted whilst the proportionality assessment is made, all the data should be secured from the beginning.

The securing of data is usually done through the copying of those data. But, it is still unclear if the copying of the electronic data shall be made only when the seizure of the hardware is not possible or is too burdensome—this is not specified in the legal systems that have special rules on search, seizure and freezing of electronic data. Once the electronic data are copied, adequate measures shall be put in place to avoid manipulation of those data and thus grant their authenticity, either by using special software, passwords, or encryption techniques. This is one of the core points for the assessment of these electronic data as evidence but, despite its importance, legal rules and guidelines are lacking in general.

Finally, the freezing of electronic data would amount to blocking the access to them. At least this is the way the freezing order of computer data is understood in the Belgian system, but the terminology used is not uniform in this point. It can be ordered in parallel with the securing (copying) of those data in order to avoid their distribution—for example, child-pornography images or “hackertools”. This measure of blocking or freezing electronic data (or whole webpages) has a different objective and aim as, for instance, the freezing of assets: even though the same term is used, its meaning is quite different.

In sum, the reporting countries inform that computer data preservation orders, as well as computer searches and seizures, are widely used in practice, mostly by the analogical application of the traditional rules on search and seizure and of freezing goods. These rules, as they have a spatial and object-oriented approach, are not always suitable for the accessing and securing of stored data or real time data flows, which do not fit into the category of movable object. The rules on search on seizure are clearly insufficient to address the problems of extended computer network searches and remote searches. Even if such lacuna might have been filled by the jurisprudence, there is still a need for more legal certainty in the regulation of measures that may interfere with human rights in a very intrusive way.

(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?

This question was answered generally before, in section (3)(5), as most reporting countries do not differentiate their cooperation for information building and for criminal investigation purposes. In general, being bound by a contract to their clients and having the duty to protect their privacy, telecom companies or service providers should not provide data unless required formally by the relevant judicial authority. In practice, this legal pathway has been often circumvented, as seen in the practice in the USA, by direct access mechanisms, and by special agreements between NSA and service providers.

Apart from these practices, most countries inform that telecom companies and service providers are obliged to cooperate with judicial authorities, provided that the data are requested in a motivated judicial warrant or production order. The deadline to comply with the judicial order varies, and it is usually determined in the judicial request, taking into account the type and extension of data required. An issue that is still unclear, and

---

59 The “quick-freezes” are regulated in art. 35 of the Cybercrime Convention of 2001, and for the effectiveness of this measure, and in general the rapid judicial cooperation, the Convention provides for the establishment of 24 hours/7 days a week contact points to deal with these requests. In how far these contact points are effectively working is not clear.
needs further study, is to what extent these telecom companies are legally bound to cooperate when they are in the position of suspect or defendant, in countries where corporate criminal liability is regulated.

Concerning the consequences of non-compliance with the obligation to cooperate, all reporting countries, except Japan, mention the possibility of imposing pecuniary fines —administrative or criminal— on the company or person whose cooperation was requested (in Belgium, e.g., the fine can be of up to 20,000 euros), and even criminal custodial penalties —for offence of disobedience or obstruction of justice— for periods of one year (Croatia and Belgium) or two years (Turkey). Obviously, custodial penalties can be imposed only on natural person, but the reporting countries do not explain who would be the person to be held criminally liable if a company does not comply with a production order or judicial request. It appears that the person who has access to the data or the passwords to make those data accessible is the one who can be coerced by the threat of custodial criminal penalties, but it is uncertain if other persons or representatives of the company can be also held liable for the offence of non-cooperation with the judicial authorities. In Sweden, the breach of the legal duty to cooperate not only can cause civil liability but also can lead to prohibiting the service provider from continuing its business.

None of the country reports mentions cooperation problems with telecom companies located in the same country, and it is more difficult to assess to what extent companies located abroad can be forced to cooperate (as stated by the Argentinian report).

One point that can explain the smooth cooperation of telecom service providers with judicial authorities is the payment of the costs. For example, the Finnish report indicates that until now there have been no problems of non-compliance with judicial requests or with the telecom companies’ obligation to retain data. Such good level of cooperation in practice may be explained by the fact that Finnish law expressly provides that companies are entitled to compensation of costs. In Belgium, service providers and telecom companies are also entitled to be reimbursed for their expenses, being the investigating judge competent to check the billing of the companies for their services, which are legally fixed and charged to the budget of the Ministry of Justice. In the USA, private companies also charge the costs for complying with data requests, and in fact the billing of these companies show the enormous amount of requests that have been complied with. Belgian legislation also foresees the possibility of reducing the payment to the companies, if the request for cooperation is not adequately carried out. Belgian law still includes another measure to encourage or force compliance with the legal obligations to retain data and to cooperate with criminal judicial authorities: telecom operators are obliged to disconnect those other service providers or final users that do not comply with their legal obligations (see p. 56). In the USA AT&T, for example, said it collected during one year 8.3 million US dollars for the services provided to law enforcement agencies, which gives an idea of the dimension of the cooperation activities between the telecom service provider and the law US law enforcement agencies.

The workload generated by police and/or judicial requests has moved these companies to establish special units to coordinate the work with judicial authorities, as well as to execute and supervise compliance with their requests (e.g., Belgium, Spain, USA). Without the right to be reimbursed for those costs, the duty to cooperate with judicial authorities will be ultimately paid either by the shareholders or by the customers—which will see their bills increased.

(4) May law enforcement agencies apply video surveillance? Can they oblige natural or legal persons to cooperate?

To understand correctly the answers provided in the national reports to this question, it is necessary to distinguish three types of situations: 1) use of video surveillance by law enforcement authorities in public spaces, either for prevention/security or for a precise criminal investigation; 2) video surveillance by law enforcement authorities in private spaces; and 3) video surveillance carried out by private persons or entities in public or private spaces.

All reporting countries inform that in their countries law enforcement agencies use video surveillance in public spaces. The question concerning fixed or movable cameras installed for building up information positions or to provide security in the public spaces was mainly answered above, in section (2)(1). Therefore, we will focus here on the use of video surveillance as an investigative measure within a criminal procedure. This

60 According to the report on USA, the bills of law enforcement requests of AT&T in one year were as high as 8.3 million US dollars.

61 On this topic see the interesting special report by G. Paolo "Judicial Investigations and Gathering of Evidence in a Digital Online Context", precisely pp. 209-225, with a special focus on the US, Canadian and Italian systems.
means that the measure is ordered once there are indications of a crime in a certain place, and the surveillance is directed to observe a certain place or a certain person. Taking pictures is not considered usually as video surveillance. More complex is to find out when we are in front of a measure of video surveillance, as some countries require, for identifying it as a measure of video surveillance, that there is a systematic surveillance of a place/person with a continuity of at least five consecutive days. This is the case, for instance, of Belgium, where shorter filmed observations of a suspect or a place do not fall under the definition of video surveillance (observation systématique) and thus are not subject to the same requirements.

The requirements for this investigative measure vary greatly. In some countries, a judicial warrant is required (Austria or Belgium) and is limited in time or allows only for offences sanctioned with a minimum custodial sentence (for example, in Austria, higher than 1 year). Other countries do not require a judicial authorisation as long as the surveillance is done in public spaces (e.g., Croatia, Finland, Italy, Spain, Turkey, USA). The USA system considers that activities developed in public places are not protected by the Fourth Amendment and therefore video surveillance in such spaces does not amount to a “search” and does not require a judicial authorization. Equally, the use of facial recognition technology in relation to the images of persons recorded in public spaces does not require a judicial authorization. This approach has been criticised on the ground that, although citizens may not expect privacy in public places assuming that they can be observed by others, there is a great difference between being seen or visually observed and being under a technologically assisted surveillance, via cameras or tracking devices, in a public space. In this regard, people have the logical expectation no to be traced, “observed” or recorded with such electronic and digital devices. Not only the level of intrusiveness is absolutely different, but also the secrecy of those measures cause an alteration of the notion of reasonable expectation in a public space62. Apropos of this, the ECtHR has held that the systematic or permanent nature of recording constitutes in itself an interference with the individual’s private life, even if the monitored activities are carried out in public63.

To fully understand the use of this measure and evaluate it from a comparative perspective, it would be necessary to know the concept of public space utilized by each legal system, something which we are not able to define here64. Obviously, the invasion of privacy will be different if the filing takes place in “open fields” or in semi-public places like a hospital. The same applies to the meaning of “video surveillance”. We have departed here from the idea that video surveillance means filming or recording images, but without acoustic recording. Despite the different scope and the problems implicit in defining the features and scope of this measure, it is important to underline that video surveillance is used in all the reporting countries in public spaces within criminal investigations, either through fixed or movable cameras.

More complicated is to determine in which countries and under which conditions is the use of video surveillance in private spaces permitted. Secret videotaping in a home or other private space in the USA requires a so-called “super warrant”, and can only be granted for certain serious crimes, listed also for wiretapping. Austria’s report indicates that installing cameras in private spaces is not allowed, but an undercover agent within operations against organised criminal groups can do the filming in those spaces. This would apply also to Spain. In the USA, some federal courts allow the secret installation of audio or video monitoring devices in a suspect’s private dwelling without a judicial warrant if the police have an informant present in the house during the surveilled conversation or activities, although several US States require the police to secure a judicial warrant before sending a wired informant to a house65. Subject to judicial warrant, Croatia and Belgium allow video surveillance in private premises as a special evidentiary action, limited to a certain list of serious crimes. Finland and Italy also provide for this measure, although in Italy—according to a

---

62 See G. Paolo, p. 244 ff.
63 ECtHR judgment Rotaru v Romania, of 4.5.2000, Appl. no. 28341/95, although this case deals precisely with the right to access and have destroyed the secret files containing the systematic surveillance and the criminal record of a person engaged in political activities during the dictatorship regime. The Strasbourg Court does not define here what are the rights of privacy or anonymity for individuals in private spaces, because recognizes a violation of art. 8 ECHR upon the lack of sufficiently foreseeable legal provision to carry out such surveillance, and the lack of efficient remedy to challenge its lawfulness. On this decision see also L. Bachmaier, Criminal investigation and the right to privacy in the case law of the European Court of Human Rights, Lex et Scientia, n° XVI, vol. 2/2009, Bucharest, pp. 9-29
64 The approach towards the protection of the privacy in the public spaces is quite variegated, as is the consideration of what is a public space. See for example, G. Paolo, pp.221 ff.
65 Following the dissenting opinion of Justice Harlan and Justice Douglas in the USSC decision United States v. White, 401 U.S. 745(1971), as states the USA report, p.52.
decision of the Italian Constitutional Court—only for “communicative behaviour”, whilst “non-communicative behaviour” cannot be recorded. In this country, it appears that recorded images will not have evidentiary value.

Finally, regarding the role of private entities or persons in the execution of the video surveillance measure, we have to address two questions. First, if they can be obliged to cooperate with the law enforcement authorities in the video surveillance. And second, if private persons can undertake video surveillance by themselves, and in such case, if they could be obliged to provide the images obtained to the law enforcement authorities and if such films would have evidentiary value.

Private persons or entities can be asked to cooperate with the police in carrying out a video surveillance in many different ways. For example, they could be asked to use their premises, because from their windows they can see the home of the suspect or a certain public space where the suspect hangs out. The cooperation could also consist in allowing the installation of a camera in the façade of a private building; or in giving access to certain computers to secretly activate the web-cam and use a private computer as a surveillance home camera; or in using the satellites of certain companies to make surveillance over a certain territory, as it is often done by state security and defence departments using their own satellites. There are many other conceivable forms of cooperation: for example, to ask a private person to carry a hidden filming device to video record private or public spaces. All these examples demonstrate that the answer to the obligation to cooperate will depend of what kind of cooperation is legally required or foreseen. However, the country reports countries do not go into such details.

Most reports indicate that there is no special obligation for private companies or persons to cooperate with law enforcement authorities in carrying out a video surveillance. An exception is Turkey, where, under the Law on internet Public Use Providers, the owners of the so-called internet cafés are obliged to install cameras and video-record the premises that provide public internet use, but this type of cooperation lies within the prevention rather than the criminal investigation field. No other legal obligations are reported, although the images that have been recorded by private actors and that might be relevant for a criminal investigation can be requested via production order by the judicial authority.

(5) May or must law enforcement agencies apply audio-visual recording of interrogations (suspects, witnesses)?

Many reporting countries indicate that the legal rules on police interrogatories provide for the possibility of audio-visual recording of such interview, but the recording neither of suspects nor of witnesses’ interviews is generally mandatory. For example, in Finland, since 2004 law enforcement authorities can videotape all interrogations, totally or partially, but must record the interrogations of the injured party and of vulnerable or future unavailable witnesses66. In the USA, while there is not any general obligation at the federal level, some states establish the mandatory recording of the suspect’s interviews (for instance, Missouri, since 2009) and some other states even require the exclusion of a confession that was not electronically recorded67. In practice, despite the fact that it is not legally required in many states, there is a growing practice of recording custodial police interrogations of suspects. Croatia requires that the first suspect’s interview is audio-video recorded (art. 275.2 CPC) and provides also for the obligation to video record the pre-trial confrontation between witnesses and the interrogations of witnesses through interpreter. Italy and Turkey also make mandatory the audio-video recording of the interrogatory of the detained suspect out of a hearing. In countries where audio-video recording is not mandatory, the practice varies greatly: in some countries this measure is often used (Austria, USA), while in others the use of such procedures is not uniform or quite unknown (Colombia, Argentina, Spain). At present, the only country report that states that there is no legal provision on this issue is Brazil, although such provision is included in the draft law for police interrogations. While the video recording of pre-trial statements of adults is quite diverse in each country, many reporting countries indicate that the interrogatory of minors that have been victim of criminal offences (most frequently sexual abuses) is mandatory (Argentina, Croatia, Finland—according to the new CPC that enters into force in 2014—and Turkey).

In an information society, where the use of ICTs is so much spread and present in all areas (economic, social, cultural, legal, or political), it is somewhat surprising that pre-trial interviews of suspects and witnesses are not, as a rule, video-recorded in all countries, and that most countries continue using written

66 See the Finland report, pp. 5-6.
67 See the USA report, p. 66.
transcriptions of oral pre-trial statements. To secure the evidence, it might be useful to apply a mandatory video-recording, although the automatic recording of all pre-trial statements may have an adverse impact on the principle of immediacy and the significance of the confrontation clause. This can perhaps explain why some legal systems are still reluctant to apply extensively the audio-video recording of pre-trial interrogatories, fearing that these may ultimately render the trial just a rubber-stamping stage of what has happened at the pre-trial stage.

4. 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?

The use of ICT in the gathering of evidence in the criminal investigation has been addressed within the previous section (3), dedicated to the collecting of criminal evidence. For this reason, we will not deal here with the rules on collecting of ICT evidence, but mainly with the integrity and admissibility of ICT evidence. We must also take into account that questions 2–5 of this section can be to some extent overlapping with this first question on evidence: if this general question about the existence of rules on evidence is answered in the negative—i.e., if there are no rules on evidence regarding ICT-related information in a country—the next four questions will also probably be answered the same way.

There have been lengthy discussions on the reliability and admissibility of ICT evidence, due to the possibility of tampering it and the easy way it might be manipulated. This discussion is not new. In Spain this was a controversial issue back in the 1970s and early 1980s when the first audio and videotapes were presented as evidence in the courts. Traditionally, Continental-European codes of procedure listed the means of evidence that could be produced and admitted at trial, and as those new technological evidentiary elements were not included in those lists, many courts initially considered them inadmissible, sometimes claiming that they were not reliable because they could be manipulated. The initial rejection of technological means as evidence has been slowly been overcome and the courts have tended to assimilate the ICT evidence to documentary evidence68. In general, it can be stated that the issue of the admissibility of legally obtained of ICT evidence is a question of the past. The authenticity of the evidence shall be checked and proofed if questioned, but the argument about manipulation will not lead to the exclusion of ICT evidence.

As has been already mentioned, the procedural legal framework in most countries has not been updated to address and regulate properly the use of ICT in criminal proceedings. This is also the case when it comes to the rules on evidence. For example, Argentina, Belgium, Brazil, Croatia, Italy, Japan, Turkey and Sweden do not have specific evidentiary rules regarding ICT-related information. The general principles of presumption of innocence and in dubio pro reo and the general rules on collection, admissibility, production, exclusion and assessment of evidence are also applicable to the ICT-related evidence. The general rule that the evidence must be relevant and material to the case, reliable, and the defendant has to be granted the right to confront evidence and cross-examine witnesses, applies also to ICT evidence.

The lack of special evidentiary rules for ICT-related evidence, according to the reporting countries, does not pose special concerns. Some countries do not have a complete regulation regarding ICTs and evidence but only single provisions that address precise aspects. Most countries have special statutory or case law rules that apply to the requirements of telephone tapping (e.g., the need to present the original tapes, or the requirement that the recording is not cut, as in Spain). Other rules relate to DNA data protection and exclusion of evidence when the matching of samples have not been done following a certain protocol; or to the admissibility and evidentiary value of audio-recorded pre-trial statements. Therefore, even if the reporting countries do state that there are no special evidentiary rules for ICT-related information, in practice in many countries the case law has defined certain requirements that are relevant for the admissibility and the assessment of ICT evidence.

Among the countries which have specific rules for ICT evidence, we can mention the following. The USA have certain provisions regarding the chain of custody to preserve the integrity of ICT evidence. In Colombia the rules on documentary evidence are applicable to ICT evidence. In Finland, where the exclusionary rule of evidence generally does not apply, there is a special provision declaring that a video-recorded hearing is admissible as evidence. Belgium has some rules on the storing of computer data. In the Netherlands, there

---

68 Although, as the Belgian report states, there are still certain courts (Tribunale correctionnel d’Anvers of 25.10.2004) that are reluctant to admit electronic evidence or even TV images, because they might have been manipulated and thus are not reliable enough. See Belgian report, p.73.
are no general exclusionary rules of illegally obtained evidence, but there is a special provision applicable to
the interception of conversations with persons who enjoy a special confidentiality protection—as, for
example, lawyers—which shall not be admitted as evidence. Dutch law contains also strict rules on technical
tools in the criminal procedure, according to which the court have to check if those technical requirements
have been met when assessing the reliability of the evidence. The Austrian CPC has some rules on evidence
that, even if they are not exclusively provided for ICT evidence, have special relevance in the context of ICT-
related information—for instance, rules dealing with the safeguards of confidentiality, the applicable rules on
data protection, or the obligation to destroy certain categories of data intercepted. Moreover, the Austrian
report informs about the guidelines issued by the Ministry of Interior (Geheimschutzordnung) regarding the
copying, storing, recording and securing the integrity of electronic data, to comply with the Data Protection
Act. China has special rules on evidence regarding ICT-information in the Death Penalty Evidence Rules,
which not only contain a list of electronic means that can be used and admitted as evidence, but also
instructions about the storage, the control of its reliability and the form of collecting it; these rules seem to be
applicable to all types of criminal proceedings.

(2) Are there any rules on integrity (e.g. tampering with or improper processing) and security (e.g.
hacking) of ICT-related evidence?

The integrity and authenticity of ICT related information has a direct impact on the evidentiary value of such
materials, its reliability and consequently its assessment. Electronic evidence might be easily modified,
overwritten, deleted or tampered. This is why rules and protocols on safeguarding the integrity of this type of
evidence are of the outmost importance. This assertion is valid for any kind of evidence. However the
problem we face here is that the traditional measures and safeguards to preserve the integrity of evidentiary
materials are not suitable for computer data, which can be very quickly deleted and altered, sometimes
without leaving traces of such manipulations. This is the reason why securing and freezing the data seized
are essential—for example, using the device called write-blocker, to prevent alterations being made to the
original data; or creating a “bit-for-bit” copy of stored information.

Proving the integrity of digital evidence should demonstrate: 1) that the digital information obtained from the
device is a true and accurate representation of the original data contained on the device (authenticity); 2) that
the device and data sought to be introduced as evidence is the same as that which was originally discovered
and subsequently taken into custody (integrity)\(^6\)

The countries reporting to have certain rules about the integrity of ICT-related evidence are: Colombia,
Croatia, Italy, the Netherlands and USA. Thus, the Netherlands regulate strictly the technical tools to be used
to protect the traceability of data as well as to avoid the danger of data being tampered (art. 126 Decree of
2006 on technical tools in criminal procedure)\(^7\); if those rules are not respected, the court may apply the
exclusionary rule of evidence on the ground of lack of technical reliability. China has legal provisions on
collecting, storing and duplicating ICT-evidence. Colombia indicates that they use the formats SHA-1 and
SHA-256 to grant authenticity. In Italy, the court can order to apply technical controls or securing measures to
grant the digital integrity of the electronic evidence, although the law does not foresee which these measures
shall be. Croatia has special rules on electronic evidence and for presenting audio-video recorded pre-trial
statements at trial. The USA provides for a complete set of rules aimed at the preservation of the chain of
custody, and the party proposing the admission of the evidence must show that there has been evidence
continuity or chain of custody\(^8\).

Evidence continuity is typically a question of fact, while the chain-of-custody process is the mechanism
applied for maintaining and documenting the chronological history of the evidence as it moves form one place
to the other\(^9\). Finally, other countries report that have special rules to preserve in general the chain of
custody of evidence, and precisely with regard to DNA data, but not specifically for ICT-evidence (Brazil,
Spain).

---

\(^6\) UNODC Comprehensive Study on Cybercrime, p. 158.
\(^7\) See Dutch report, p.24.
\(^8\) For the use of digital evidence in court and the need to prove the continuity and the chain of custody, see Digital
Evidence in the Courtroom: A guide for Law Enforcement and Prosecutors, of the U.S. Department of Justice, published
UNODC Comprehensive Study on Cybercrime, p. 158.
(3) Are there any rules on admissibility (incl. the principle of procedural legality) of evidence that are specific for ICT-related information?

All reporting countries inform that there are no special rules on the admissibility of ICT-related evidence, and that the general rules on exclusion of evidence apply. The report on Colombia indicates that the ICT-evidence has to present some indications on the authenticity and integrity of the evidence, showing, for example, that the standards and principles used for example by the FBI or the scientific working group on digital evidence (SWEDGE) have been respected. However, it is unclear if these standards are a strict requirement for the admissibility of the evidence or merely criteria to be taken into account for the assessment of the evidence.

Considering that electronic or digital evidence has often to be obtained abroad, common rules on the collection, as mentioned above, would facilitate the admissibility in the forum state. However, since such an harmonization is not easy to achieve, and even less at a global level, it would be desirable to agree on certain principles and standards for transnational criminal proceedings, in order to avoid that the evidence obtained abroad is finally not admitted by the trial court, arguing that it does not comply with the domestic procedural requirements. The “principle” that the difference in regulation should not constitute a ground to deny the admissibility of evidence is included in the Proposal for a Regulation on the European Public Prosecutor’s Office, precisely to avoid the obstacles for the cross-border evidence transfer and admissibility. The questionnaire sent to the rapporteurs did not specifically address the issue of admissibility of evidence collected abroad—or located abroad—and therefore we only can underscore here the importance of setting some general principles for cross-border evidence, and also for cross-border ICT-evidence, which has acquired an increasing importance in prosecuting all types of crimes.

(4) Are there any specific rules on discovery and disclosure for ICT-related evidence?

In general, all country reports state that there is no specific regulation for ICT-related evidence, and that the rules regarding the access to file and the right of the defence to examine the prosecution materials apply. It may be inferred that the answers of the country reports have in mind non-classified ICT-evidence, for none of the reports—except USA—mentions the possibility of delaying or excluding some data if it is necessary to protect the source or there might be a risk for the prosecution if full disclosure is allowed. Therefore, the answers to this question have to be interpreted generally as not dealing with the issue of special provisions for secret or classified information.

In the USA, secret interceptions and searches carried out under the Foreign Intelligence Surveillance Act (FISA) shall be disclosed, unless the government claims that the disclosure of the wiretaps, electronic communications or video recordings would constitute a revelation of state secrets or other classified information. In such case, the court must proceed under the rules of the Classified Information Protection Act, which exclude some parts of the classified information and provide the defence with a summary of the content or foresee a hearing in camera with a security cleared defence lawyer.

(5) Are there any special rules for evaluating (probative value) ICT-related evidence?

All the country reports inform that there are no special rules for the evaluation and assessment of the ICT-related evidence. However, it is interesting to see how the USA’s exclusionary rules on “hearsay” are applied to the ICT-evidence, as will be seen in the next section.

73 For a short summary of the main problems regarding the collecting and admissibility of evidence in EU cross-border proceedings, highlighting the problems for the defence rights, see M. Simonato, pp. 18 ff.
75 See art. 30 of the Proposal for a Council Regulation on the establishment of the European Public Prosecutor’s Office, COM(2013) 534 of 17.7.2013
77 See USA report, p. 69.
5. ICT in the trial stage

(1) How can or must ICT related evidence be introduced in the trial?

The question posed here is certainly broad, as it refers to the way in which the ICT-related evidence must be introduced in trial, without making any distinction on the different types of information or evidence that have been collected or recorded using ICTs. At such general level, focusing only on “how” the evidence is to be produced at trial, all country reports—save USA—either refer to the rules on documentary evidence or state that the evidence recorded on a tape or film, or stored in a computer, shall be presented by playing such recordings, or showing the computer data by using the computer at court. Additionally, the audiotapes and the computer data can be accompanied by the written transcription, being unclear if such transcriptions are always mandatory or not. If the ICT-related evidence consists in a film, the majority of countries inform that it can be played in the courtroom. Some countries, as China, require presenting at trial the original storage device and, if the authenticity is discussed, the expert shall present the electronic evidence. Moreover, the authorities handling the recorded materials may be questioned about the collecting, storing conditions of such material as well as the rules applied to preserve the chain of custody.

The USA, due to their special rules on hearsay evidence, have a different approach. In this country, “hearsay” is defined as a statement, whether oral or written, or even an assertion by gestures, which was made outside of the trial, but is introduced in the trial to prove the truth of the matter asserted. As a consequence, any statement made outside the trial, whether as a result of interrogation or of a legal interception of communication, is “hearsay” evidence. In the USA, as a rule, recorded materials will be presented at trial through witness testimony. For any tape recording, or business record showing trap and trace or pen register information admissible, the officers conducting the wiretap or bugging operation must testify as to how they carried out the surveillance, to the chain of custody and in general to the safeguards adopted. However, the hearsay rule has numerous exceptions. For instance, statements recorded in audio-video tape can be directly played at trial. This is the case for the statements made by minors that have victims of sexual abuses.

If we enter into more details, it should be explained under which circumstances the recorded pre-trial statements can be played or read out at trial. None of the country reports, with the exception of the USA, inform about the conditions and circumstances that allow the production of filmed pre-trial statements, or reading out the transcriptions of such declarations of the victim, the defendant or the witnesses. In the USA criminal procedure, the recorded pre-trial statements of witnesses are exceptionally admissible (exceptions of “excited utterance”, “present sense impression”, statements for the purpose of medical treatment, or statements of existing mental, emotional or physical condition, business records exception). Under these exceptions, the courts have admitted as evidence, for instance, the tape-recorded statements made by a woman reporting to the police on the phone while she is being battered by her husband, if she was unable to testify in court.

For a better assessment of the role of the ICTs as evidence, it would be necessary to further analyse which are the circumstances that allow to hear and/or see those pre-trial recorded statements and under which conditions they can be assessed as evidence. It would be interesting to observe if the pre-trial recorded confession is admissible at trial when the defendant decides to remain silent at the courtroom, or when the witness invokes at trial his/her right not to testify after having declared during the pre-trial stage.

From the information provided by the reporting countries it is possible to infer some clear conclusions. First, there are still many countries that have not included special provisions for the presentation of ICT-related evidence at trial, and simply rely on the traditional rules on documentary evidence, which are not always perfectly applicable. Second, it should be precisely stated how the ICT evidence is presented, clarifying when and to what extent written transcriptions (sometimes very costly and time consuming) should be required. And finally, it would be desirable that the legal rules on presentation of ICT evidence specify when preference should be given to playing the film or listening to the audio-tapes at court, rather than hearing the testimony of the authorities who intervened in those recordings or reading out the transcriptions. In short, when the direct source of evidence cannot be heard in the courtroom, it would be preferable to watch the recorded pre-trial statements rather than questioning the officers who interrogated the witnesses or reading out the transcriptions of their statements—video recording seems to be a better and more accurate option, for they

---

78 See USA report, p. 69.
79 See USA report, p.67.
allow the judge or the jury to better assess those statements. We are aware that this option is alien to the common law procedural system, but this aspect of its procedural tradition might be perhaps rethought in the light of the advance of ICTs in the criminal procedure.

(2) Can distant interrogations (e.g. by satellite connections) be applied?

The general answer in all country reports countries is that distant interrogations are possible in the criminal trial. However, when dealing with distant interrogations during the trial, distinction has to be made between defendants and witnesses. We assume that those reports that do not make such distinction are answering only with regard to witnesses, for the majority of countries do not accept, as a rule, the holding of a trial without the physical presence of the defendant. Despite this general approach, as some countries exceptionally allow the appearance of the defendant at trial through video- or teleconference, we will address the two situations separately.

The law of almost all studied countries foresee some ways in which a witness can testify through video-link or videoconference; such possibility is usually utilized for witnesses whose physical appearance is not possible or when a witness is abroad. This is the case in Austria (art. 247a CPC), Belgium, Colombia (art. 386 after Law 906/2004), Croatia, Finland, Italy, the Netherlands, Spain, and Turkey. It must be remarked that the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 specifically provides for the possibility of holding the hearing of witnesses by videoconference, and does not exclude the holding of the videoconference during the trial (10). The same provision is also included in art. 9 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters elaborated within the Council of Europe. This Second Protocol to the European Convention of 1959 follows closely, and often literally, the above-mentioned Convention of 29 May 2000 on Mutual Assistance in the EU. In consequence, in the 47 Member States of the Council of Europe it should be possible to hear witnesses who are abroad through videoconference. In contrast with the CoE’s landscape, Japan does not foresee such possibility.

Apart from witnesses who are abroad, many of the reporting countries also allow the use of videoconference when a witness is under a special protection programme (e.g., Italy, the Netherlands, Spain or Turkey), or when it would not be possible—or it would be too burdensome—to make the witness appear physically at court. Interrogatories of witnesses through videoconferencing is also encouraged at the EU level. Additionally, as explained above, there are usually special rules for the testimony of minors who have been victims of sexual offences. In such cases, many countries do not only provide for the possibility of declaring by videoconference, but also establish the mandatory recording of the pre-trial statement. Even in a system like the USA, where the application of the confrontation clause is understood in a very strict way, the courts have admitted the use of two-way closed circuit television to avoid the child witness to appear at court and confront the defendant. It is considered that in this case a strong reason of public policy justifies the exception. New York has a statute that authorizes children victims of sex abuses to testify by video; and the state’s highest court has admitted the possibility of applying this exceptional rule to other cases, as in a case in which the victim was a 83-year-old man, who was too frail to appear in court.

With regard to the defendant, the general rule is still that trial cannot be held if the defendant is not physically present, and many countries are reluctant to change this rule, because of the risks that it could entail for the defence rights of the defendant. The presence of the defendant has been considered as an essential rule for

83 See the E.M., point 9, although in other provisions it follows the Convention of 14 June 1990 implementing the Schengen Agreement of 14 June 1985.
84 On current practical issues on transnational videoconferencing in the EU, see Council Document No. 16269/13, p. 6, cited by D. Brodowski in his report “European Initiatives Concerning the Use of IT in Criminal Procedure and Data Protection. Special report for the Preparatory Colloquium for the Third Section, note 43.
the adequate assessment of the evidence, the respect of the confrontation clause and a sine qua non condition for safeguarding the defence rights. This is the reason why, despite the new technical possibilities, only a few countries still allow the appearance of the defendant at trial through videoconference—according to the country reports, China, Italy, the Netherlands, Turkey and Spain, which foresee the possibility of hearing the defendant through video link. In China, this possibility is foreseen for appeal and review proceedings, and is reported to be widely used in practice due to the vast geographical dimensions of this country. In Italy, where also trials in absentia are exceptionally accepted, the law provides for the possibility that the defendant appears at trial via video link if there are serious reasons for security. This provision endeavours to deal with problems of mafia-related crimes, in which the complexity of the crime, the serious risks for security and for absconding justify that the defendant is not brought to trial, but is kept in prison and follows the whole procedure through video link. Turkey permits that the defendant appears through videoconference only for the hearing on remand on custody, but not for the trial itself. In Spain, where also the general rule is that the trial cannot be held if the defendant is not present in the court room, in exceptional terrorism-related cases in which the defendants’ behaviour obstructed the normal development of the trial, the courts have accepted that the disrupting defendant was transferred from the courtroom to an adjoining room equipped with video link. This solution was not specifically foreseen by legislation but adopted by the courts on their own initiative and later declared constitutional by the Spanish Constitutional Court.

(3) Can digital and virtual techniques be used for the reconstruction of events (killings, traffic accidents)?

All country reports state that digital and virtual techniques can be used for the reconstruction of events, although in many of them the possibility is not regulated precisely. This is the case for example of Argentina, Brazil, Croatia, Finland, Japan, Italy, Spain, Sweden and Turkey, where either there is no regulation but the reconstruction of events is allowed as long as it is not forbidden, or the traditional rules on reconstruction of events do not indicate which are the means or devices that are to be used or excluded for this investigative or evidentiary measure (as, for example, the regulation on the Tatenrekonstruktion in Austria, arts. 149-150 CPC). Several countries report that the regulation on the reconstruction of the events is not contained in the CPC but in the rules on professional judicial experts or forensics (e.g., Croatia and Turkey).

(4) Can audio-visual techniques be used to present evidence at trial (in its simplest form: pictures and sound)?

This question was partially answered under question (5)1, when dealing with the issue of how the ICT-related evidence could be presented at trial. Those country reports that responded that the ICT-related evidence could be presented by playing the film, or listening to the audiotape, answer the present question also in the affirmative. Nevertheless, the present question goes beyond the one posed under (5)1, because it refers precisely to the use of audio-visual techniques to present evidence in general, and not only ICT-related evidence.

Reading the country reports, the general conclusion is that audio-visual techniques can be used to present evidence at trial, either because it is not prohibited (the majority) or because it is specifically foreseen by the law. In practice, the use of these techniques varies greatly from country to country, as well as within the same country the practice differs depending on the courts. Most rapporteurs state that their use depends ultimately on the existence of the adequate equipment (e.g., Japan, Spain), the type of evidence (if it needs the audio-visual techniques or not), and the complexity of the case. In continental European countries, unless the kind of evidence strictly requires the playing of the film, the listening to the audiotape, or the showing of some computer systems, programs or data, the lawyers usually do not resort to audio-visual or Powerpoint presentations in their defence. In this aspect, the practice in the USA appears to be more adapted to the use of modern technologies in the courtroom. The number of federal courtrooms that have been certified as “high technology courtrooms” has increased rapidly, and the two-way video technology had been authorized in courtrooms in 29 states by 2003. Moreover, the lawyers frequently use ICTs and PowerPoint presentations not only for presenting allegations or explaining evidence, but also for presenting their concluding arguments.

(5) Can criminal “paper” case files be replaced by “electronic ones”? Are there any developments towards digitalising of the trial proceedings?

At the time of writing this report, none of the reporting countries has gone so far in the implementation of the e-justice as to reach the substitution of paper case files by electronic files completely. However, with the exception of Japan, all the reporting countries state that there have been approved digitalization programs that should progressively lead to a gradual transition towards electronic judicial files, but there are scarce
data on the effective implementation or progress of such programs. Belgium regulated the electronic proceedings by Law of 10 July 2006, together with the project “Phenix”, to make the transition to electronic justice. The law established a peculiar principle: each file should be either completely electronic or completely in paper, not being admissible the digitalization by pieces or parts of the file, and rejecting also the possibility of having hard copies in addition to electronic files. The project was not only complex but required also a huge financial investment, and hence has ended up failing. Nevertheless, the Ministry of Justice approved another project that should be implemented in January 2015. Similar problems regarding the implementation of the digitalization of the administration of justice are reported by other countries.

The USA, once again, seems to be more advanced in the use of ICTs and modern technologies in the justice system. The USA report informs that litigators commonly utilize electronic filing programmes, electronic docketing and online case managements, in addition to e-mail communications with the court. There is also currently a discussion about introducing virtual trials, although with the restrictions that the rules on confrontation and right to cross-examine witness require. Until now this is only a topic for discussion and the future will show if it becomes a reality.

Concerning partial digitalization, most countries report advances towards the e-justice, at least in some areas, some judicial acts, or some stages of the proceedings. Many of them have started by digitalizing some documents and information (at the EU level, see the e-justice portal). Others have digitalised the Supreme Court or Higher Court’s decisions, while others have already all judgments in digital form. This is an important step forward, but this is not yet sufficient to speak of an electronic justice—it is rather a way to improve access to information through the use of electronic databases.

Austria informs that digitalization has been implemented at the police level and also with respect to the Constitutional Court’s case files. The Netherlands provides already for reporting petty offences to the police electronically. In Spain, certain offences can also be already reported electronically. Many documents are digitalised in Italy, and in Spain advocates have already the possibility of presenting documents and receiving notifications electronically, either directly or through a court representative. At the EU level, there is a recent pilot project to dematerialize certain international cooperation proceedings, precisely the European Arrest Warrant Proceedings, comprising France, Germany and Spain.

In sum, there are many programmes with the aim of digitalizing the judicial proceedings but the reality demonstrates that the e-justice, the e-file and the e-proceedings are still a distant reality. This weak and slow improvement contrasts strikingly with the digitalization of other public administrations, such as tax agencies or administrative proceedings. Issues of cyber security and dangers for confidentiality are usually invoked for not advancing decidedly towards the complete dematerialization of justice files that contain not only data that are personal, but often sensitive and confidential. For the position of the defence, the digitalization of the proceedings could facilitate access to the file, especially in complex cases with a large amount of documents, and could reduce time-consuming visits to the courts by lawyers or their representatives.

---

86 This pilot project is called e-CODEX and has started in late 2013. See the EU report of D. Brodowski, p.8.