The European Legal Framework on Electronic Evidence

Mifsud Bonnici, Jeanne Pia; Tudorica, Melania; Cannataci, Joseph A.

Published in:
Handling and Exchanging Electronic Evidence Across Europe

DOI:
10.1007/978-3-319-74872-6_11

Publication date:
2018

Chapter 11
The European Legal Framework on Electronic Evidence: Complex and in Need of Reform

Jeanne Pia Mifsud Bonnici, Melania Tudorica, and Joseph A. Cannataci

Abstract More and more, "electronic evidence", defined as "any of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device", plays an important role in criminal trials. This is not surprising given that most of the activities we take part in daily are captured in an electronic way, for example, our electricity consumption is registered electronically by smart meters, our smart mobile phones store information on our calls, messaging, Internet behavior, lifestyle choices, etc., all of which may have some potential probative value in a criminal trial. Apart from, or because of, its particular nature, electronic evidence is not necessarily linked to the same territorial jurisdiction as where an alleged crime would have taken place or is being investigated. This paper focuses on three aspects of this cross-border nature: (a) where it may be due to the information provider "recording" the information; (b) where the actual digital information is stored; (c) where the crime itself has a cross-border nature. This paper reflects on these three effects of this "cross-border" nature of electronic evidence when regulating electronic evidence in the criminal law process. This paper shows how current national and international legal frameworks are insufficient to meet with the current needs. Further it is argued that solving the current shortcomings is not merely a matter of introducing new agreements but is more complex, needing new theoretical frameworks and the collaboration of a large variety of actors.

11.1 Introduction

With most of our lives organised online and by using the latest technologies we rely on Information and Communications Technology (ICT) and use it in our daily lives to interact with our friends, families, colleagues, even with the government, we use it to share and store information, conduct our business, etc. The systems

J. P. Mifsud Bonnici (✉) · M. Tudorica · J. A. Cannataci
University of Groningen, Security, Technology and e-Privacy (STeP), Groningen, The Netherlands
e-mail: g.p.mifsud.bonnici@step-rug.nl; m.tudorica@step-rug.nl; j.a.cannataci@step-rug.nl

M. A. Biasiotti et al. (eds.), *Handling and Exchanging Electronic Evidence Across Europe*, Law, Governance and Technology Series 39,
https://doi.org/10.1007/978-3-319-74872-6_11

keep our economies running. Consequently, we leave digital traces everywhere. Therefore, the evidence we may need to bring to Court is increasingly in electronic form. This is especially the case in criminal matters. Evidence in criminal cases is how the facts are established to prove an individual's guilt or innocence. This evidence may be traditional (physical evidence, a murder weapon for example). However, increasingly, evidence nowadays are in electronic form (for example mobile mast records showing the location of a suspect at the time of the murder). This is not surprising given that most of the activities we take part in daily are captured in an electronic way, for example our electricity consumption is registered electronically by smart meters, our smart mobile phones store information on our calls, messaging, internet behaviour, life-style choices etc., all of which may have some potential probative value in a criminal trial. Apart from, or because of, its particular nature, electronic evidence is not necessarily linked to the same territorial jurisdiction as where an alleged crime would have taken place or is being investigated. Data may for example be stored in a cloud service that is located in another jurisdiction. Moreover, criminal activities are also increasingly conducted using ICT and perpetrators rely on digital technologies to perform their activities (for example cybercrimes). All this evidence in criminal cases needs to be collected by enforcement authorities, preserved, used in criminal proceedings and possibly transferred or exchanged (cross-border) between authorities.

Evidence may come in different forms. As described in other parts of this Volume, there are various definitions of electronic evidence and in some cases the term is used interchangeably with the term 'digital evidence'. However, we use the term *electronic evidence*, which is defined as "any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device".[1] We therefore take a wide approach to electronic evidence to include: physical or traditional (not electronic) evidence such as a murder weapon or the bloodstain of the victim, which may be digitised for example by taking a digital photo of the murder weapon; evidence born in an analogue format (videotape or vinyl), which may be digitised and entered into a digitisation process acquiring digital status; and evidence originally born digital as created by any digital device (computer or computer like-device). All these types of evidences are considered as 'electronic evidences' considering that at the end of the process they can be labelled as electronic regardless of their origin.

Because of the very nature of it, modern technologies and growing globalisation, electronic evidence may be located or stored anywhere in the world. This is especially the case in cybercrime cases, as cybercrime is a global problem that does not stop at our countries' borders, but also increasingly in crimes in general and terrorism cases. It is therefore not sufficient to say that electronic evidence is only relevant to cybercrime cases. Electronic evidence may be used in any criminal case. In criminal matters all types of electronic evidence need to be collected and handled

[1]Definition used in the EVIDENCE Project—Deliverable 2.1—EVIDENCE Semantic Structure, p. 18.

by enforcement authorities and prosecutors before they can be presented and used in Court. In investigating criminal matters, enforcement authorities need a variety of powers to collect, preserve and exchange (electronic) evidence. They might need traditional powers (interview, surveillance, etc.) but also cyber-specific powers, such as search and seizure of stored computer data, real-time collection of traffic data and interception of content data as evidence may come in the form of computer files, logs, transmissions, metadata, computer data, etc. This evidence then needs to be preserved and handled, possibly by digital forensic experts, to be presented and used in Court. To be presented and used in Court the electronic evidence needs to comply with all necessary rules, if any, including rules on admissibility. For example, in many legal systems the (electronic) evidence needs to be legally obtained, i.e. by Court order, for the evidence to be admissible in Court. As electronic evidence can be easily modified, overwritten or deleted, the authenticity of the evidence may also be questioned in Court. Like physical evidence, electronic evidence needs to be authenticated and verified.[2] A clear chain of custody is therefore of the essence.

This chapter reviews the current legal framework for electronic evidence in Europe. It first looks at the international level, examining frameworks coming from the Council of Europe and the European Union (EU). It then moves to review the position at a national level (within Europe). The review shows a complex patchwork of legislation and practices relating to electronic evidence and one that needs reform to meet the demands of the increasing use of electronic evidence in the criminal process.

It is important at this stage, before moving on with the review to discuss the use of some of the terms used in this chapter. Processing evidence in criminal matters refers to collecting, preserving, using and exchanging evidence, i.e. the chain of custody of evidence in criminal proceedings. By collection of electronic evidence, we mean the process of gathering items that contain potential electronic evidence in the widest sense, meaning search, seizure, interception and any other forms of gathering evidence by Law Enforcement Agencies (LEAs), but also capture of evidence by the private sector and any other forms of gathering potential electronic evidence. Once the evidence is collected, it needs to be preserved before it can be used during the criminal trial. Preservation is the process of maintaining and safeguarding the integrity and/or original condition of the potential electronic evidence, meaning that it needs to be stored in a secure way to safeguard against alterations, that the chain of custody needs to be logged and that access to the evidence needs to be restricted to persons authorised to process the evidence. Before the criminal trial starts the electronic evidence needs to be to be analysed, for example by digital forensic experts, and the final document or report needs to be produced before it can be used and presented in court. At any point during the electronic evidence lifecycle the evidence may thus be interchanged between various competent authorities including LEAs, digital forensic experts, courts, etc. To distinguish between the interchange

[2]United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 158.

within a country and cross border interchange, we refer to the first as *transfer* and to the latter as *exchange*. Transfer may occur between different national legal actors and LEAs in the same country. Exchange may take place between competent national authorities of different countries (cross-border exchange) in the field of cooperation in criminal matters. All the actions from collection to eventually using the evidence in court require a legal basis.

11.2 International and European Legislation and Practices

When describing whether and how electronic evidence is perceived and regulated in the EU legal framework it is important to realise that criminal law is based on national laws and traditions that differ per Member State. However, these national laws may be inspired by international instruments or may even have implemented international instruments such as EU and Council of Europe legal instruments and best practices. When describing the European legal scenario, it is therefore relevant to look at these instruments before going into the scenarios at national level.

There is no comprehensive international or European legal framework relating to (electronic) evidence. Parties involved rely on national law when it comes to the collection, preservation, use and exchange of (electronic) evidence. These national criminal laws have been written ages ago, long before there was such a thing as the internet and modern technologies that could generate electronic evidence. While it is true that some countries have adapted their legislation to include such developments, others rely on traditional criminal laws and apply them to electronic evidence as well. There are thus big differences in national legislation and approach, which makes handling transnational electronic evidence difficult. According to the United Nations (UN) Study on Cybercrime,[3] evidence rules vary considerably even amongst countries with similar legal traditions.[4] In certain countries traditional investigative powers might be general enough to apply to electronic evidence, while in other countries traditional procedural laws might not cover specific issues regarding electronic evidence, making it necessary to have additional legislation. In certain countries there are defined rules as to admissibility of evidence in Court while in other countries admissibility is flexible. In all cases legislation requires a clear scope of application of powers and sufficient legal authority for actions by the authorities involved.[5] While there is no comprehensive international or European legal framework relating to electronic evidence, few international and European

[3] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013.

[4] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 158.

[5] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 122, 123.

legal instruments and policy documents are relevant to electronic evidence. These instruments and documents may inspire national laws and practices or may even be implemented into national law. Apart from these international and European instruments and documents it is furthermore worth mentioning that Member States may also rely on bilateral and multilateral agreements between them, particularly when it comes to cross-border exchange of (electronic) evidence. We will not go into these agreements. However, it is relevant to know that these agreements may exist between countries.

The two main international legal regimes that influence national laws are the EU legal framework and Council of Europe legal instruments. The EU cannot adopt general EU criminal law, however, with the entry into force of the Lisbon Treaty and the creation of an Area of Freedom, Security and Justice (AFSJ), the EU can add important value to existing national criminal laws within the limits of its competence. However, there is no comprehensive EU legal framework regarding criminal law and none whatsoever regarding electronic evidence. There are only few EU instruments that may be directly or indirectly relevant to the collection, preservation, use and exchange of electronic evidence. The Council of Europe is highly relevant in this respect as all Member States of the EU are States Parties to the Council of Europe as well and the Council of Europe has produced several international treaties relevant to electronic evidence. The Council of Europe Convention on Cybercrime[6] (Cybercrime Convention) remains the main (and only) international treaty that defines the procedural provisions for investigating and pursuing cybercrime. Although electronic evidence may not necessarily flow from cybercrime but may also be processed in proceedings of traditional crimes, the electronic evidence may be collected, preserved, used and exchanged in the same manner in criminal investigations of both cybercrimes and traditional crimes. The EU and Council of Europe legal frameworks will be discussed in the following paragraph. It is important to note in advance the patchwork of legal instruments that authorities, particularly law enforcement, are left to operate with. This highly uncertain and politically sensitive landscape filled with legal lacunae makes cross-border cases and international cooperation difficult.

11.2.1 European Union Legal Instruments

With the adoption and entering into force of the Lisbon Treaty[7] a supranational regime for EU criminal law was introduced. Title V of the Treaty on the Functioning of the European Union[8] (TFEU) provides for the AFSJ within the EU. Based on

[6]Convention on Cybercrime [2001] ETS 185.

[7]Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community [2007] OJ C 306/01.

[8]Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47.

Article 67 (3) TFEU, with this area the EU will endeavour to ensure a high level of security through measures to prevent and combat crime, through police and judicial coordination and cooperation, through mutual recognition of judgements in criminal matters and if necessary through harmonisation of criminal laws. The AFSJ thus includes EU criminal law and police cooperation, which is further developed in Chapters 4 (judicial cooperation in criminal matters) and 5 (police cooperation) of Title V TFEU. Although it is thus true that there has been progress on the EU legal framework front, the realities are somewhat different. Judicial and police cooperation are subject to Article 4 (2) of the Treaty on the European Union[9] (TEU), which states that national security is the sole responsibility of each Member State, interpreted in the sense that the provisions regarding judicial and police cooperation are on stringent terms with sovereignty regarding national security. Even more so considering that sensitive matters can be referred to the European Council. Instruments adopted prior to the Lisbon Treaty furthermore retain their earlier status, the United Kingdom (UK) and Ireland can opt out of any of the instruments and Denmark is only bound by its commitments under the Schengen Convention.[10] Having said that, the regime has been a step forward, as judicial and police cooperation is of utmost importance regarding the collection, preservation, use and exchange of (electronic) evidence and judicial authorities and police forces across Europe tend to work together in preventing and solving cross-border

According to Article 82 (1) TFEU judicial cooperation in the EU is based on the principle of mutual recognition of judgements and judicial decisions and includes approximation of laws and regulations of the Member States in several areas including mutual admissibility of evidence between Member States (Article 82 (2, a) TFEU) and in some number areas of serious crimes including terrorism, organised crime and cybercrime (Article 83 (1) TFEU). According to Article 87 TFEU police cooperation in the EU is established involving the competent authorities of the Member States and the EU. Based on these provisions the EU may issue Directives and other measures to the extent necessary to facilitate judicial and police cooperation within the EU. The EU has adopted few Directives and other measures regarding criminal law. This includes the EU 2000 Convention on mutual assistance in criminal matters,[11] which was adopted by the Council in 2000 in accordance with Article 34 TEU and entered into force on 23 August 2005 to facilitate mutual judicial assistance between the authorities of the Member States (police, customs and courts) to improve the speed and efficiency of judicial cooperation. The EU 2000 Convention encourages and facilitates mutual assistance between judicial, police and customs authorities on criminal matters that complements and adds to the

[9]Consolidated version of the Treaty on European Union [2012] OJ C 326/13.

[10]See Chalmers et al. (2010), p. 582.

[11]Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 197/01) [2000] OJ C 197/1.

Council of Europe Convention on Mutual Assistance in Criminal Matters.[12] Based on the EU 2000 Convention Member States may request other Member States for mutual assistance. Requests might also include requests for (electronic) evidence. However, the downside with such procedures for mutual assistance is that they are time consuming as requests for mutual assistance generally take a long time to be processed, which cannot be afforded, particularly when it comes to electronic evidence that is easily altered or even deleted. In 2008, the European Evidence Warrant (EEW) Decision[13] replaced the system of mutual assistance in criminal matters between Member States for obtaining objects, documents and data for use in criminal proceedings (Article 1 (1) EEW Decision) and established the procedures and safeguards for Member States whereby EEWs are to be issued and executed. The EEW Decision was adopted to apply the principle of mutual recognition in obtaining objects, documents and data for use in proceedings in criminal matters. However, the EEW is only applicable to evidence that already exists and covers therefore a limited spectrum of judicial cooperation in criminal matters with respect to evidence. Because of its limited scope, competent authorities have been free to use the regime of Directive 2014/41/EU, the European Investigation Order (EIO) Directive,[14] when it was issued in 2014 or to use mutual legal assistance procedures that remain applicable to evidence falling outside of the scope of the EEW.[15] The EIO Directive sets up a comprehensive new system that allows EU Member States to obtain evidence in other Member States in criminal cases that involve more than one Member State. This Directive thus aims to simplify and speed up cross border criminal investigations in the EU. It introduces the EIO, which enables judicial authorities in one Member State (the issuing state) to request that evidence be collected in and transferred from another Member State (the executing state). It replaces the existing EU mutual legal assistance schemes, notably the EU 2000 Convention and EEW Decision. It needs remain to be seen how this will work given that it has only come into force on 22 May 2017.

Based on Article 1 of the EIO Directive, the EIO is a judicial decision that has been issued or validated by a judicial authority of the issuing State to have one or several specific investigative measure(s) carried out in the executing State to obtain evidence or to obtain evidence that is already in the possession of the competent authorities of the executing State. Member States are obliged to act swiftly and to execute the EIO based on the principle of mutual recognition. The EIO covers any investigative measure except for the setting up of a Joint Investigation Team

[12]European Convention on Mutual Assistance in Criminal Matters [1959] CETS 030; Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] CETS 099.

[13]Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for obtaining objects, documents and data for use in proceedings in criminal matters [2008] OJ L 350/72.

[14]Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1.

[15]Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1, Recital 4.

(JIT) and the gathering of evidence within such a team as provided in Article 13 of the EU 2000 Convention. The EIO improves on existing EU laws covering this field by setting strict deadlines for gathering the evidence requested and by limiting the grounds for refusing such requests. It also reduces paperwork by introducing a single standard form for authorities to request help when seeking evidence. The EIO may be issued in writing if it is necessary and proportionate for the proceedings and if the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case (Article 6 (1,b) EIO Directive). The Directive does not mention electronic evidence as such. However, it refers to 'data', which indicates that evidence may indeed be in electronic form. Article 13 of the EIO Directive arranges for the exchange of evidence and stipulates that the executing authority transfers the evidence obtained or already in the possession of the competent authorities to the issuing State. However, it does not stipulate how the evidence should be transferred, nor does the Directive determine how evidence should be collected and preserved. This is left to the Member States, meaning that this may vary considerably between Member States.

Other EU police cooperation schemes include the Schengen acquis, the European Arrest Warrant (EAW) and JITs. The Schengen acquis facilitates, amongst other things, police cooperation within the Schengen Area. The Schengen Area is an area without internal borders, an area within which people can freely circulate without being subjected to border control. By abolishing the internal borders, Schengen States made rules to ensure the security of those living or travelling in the Schengen Area, including tightened controls at their common external border and enhancing police cooperation. The Schengen acquis is the body of law regulating the Schengen Area. It includes the Schengen Implementing Convention and other legal instruments.[16] Title III of the Schengen Implementing Convention is devoted to police and security. To facilitate the Schengen Area and police cooperation the Schengen States introduced the Schengen Information System (SIS). SIS enables competent authorities to enter and consult alerts on certain categories of wanted or missing persons and objects. It is the largest and highly secure and protected EU database that is exclusively accessible to the authorised users within competent authorities, such as national border control, police, customs, judicial, visa and vehicle registration authorities. The EAW based on Framework Decision

[16]The Schengen acquis—Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L 239/19. See also: Regulation (EC) no 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L 381/4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L 205/63; Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1.

2002/584/JHA[17] is a judicial decision issued by a Member State for the arrest and surrender by another Member State of a requested person in conducting a criminal prosecution or executing a custodial sentence or detention order (Article 1 (1) EAW Decision). The Decision simplifies and speeds up procedures whereby EU citizens who have committed a serious crime in another Member State can be returned to that country to face justice. Like all the other EU instruments in this regard the EAW is executed based on the principle of mutual recognition.[18] Finally, and possibly most importantly, European police cooperation may include JITs, which find their legal basis in Council Framework Decision 2002/465/JHA.[19] Member States meeting in Tampere in 1999 called for JITs to be set up without delay with a view to combating trafficking in drugs and human beings, as well as terrorism. The EU 2000 Convention had already provided for the setting-up of JITs, however, in view of slow progress towards ratification of the EU 2000 Convention, the Council adopted Decision 2002/465/JHA to carry out criminal investigations in Member States that necessitate coordinated and concerted action.[20] JITs may be set up by at least two Member States for a specific purpose and a limited period based on an agreement of all the parties involved. Representatives of Europol, OLAF and of third countries may take part in the team's activities. Increasingly, this is one of the most relevant instruments for Europol to share its expertise in collection, preservation and facilitation of exchange of electronic evidence, particularly in the context of cybercrimes.

11.2.2 Council of Europe Legal Instruments

Apart from the above-mentioned EU legal instruments, there are few instruments by the Council of Europe that are relevant to electronic evidence. In fact, the Council of Europe instruments and documents are generally more authoritative than the international and EU ones. Regarding international organisations, the Council of Europe has more members than the EU and all EU Member States are States Parties to the Council of Europe as well, particularly concerning cybercrime, the Council of

[17]Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [2002] OJ L 190/1.

[18]The EAW Decision has been criticised enormously, in fact it has prompted more challenges before constitutional Courts of the Member States than any other EU law. The most important concern in this regard is related to trust, trust in the prosecutorial and judicial process of the issuing state, mainly in that there might be insufficient guarantees that the surrendered person will receive a fair trial in the issuing state. See Chalmers et al. (2010), p. 599.

[19]Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA) [2002] OJ L 162/1.

[20]On the relevance of JITs, see: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *The European Agenda on Security* COM(2015) 185 final, p. 9.

Europe provides a binding international treaty that affords an effective framework for the adoption of national legislation and a basis for international cooperation in this field.[21] In several pieces of EU legislation and policy documents it is reiterated that the Council of Europe's instruments are the legal framework of reference for combating cybercrime and that the EU legislation and policies build on those of the Council of Europe. As far as electronic evidence is concerned, several Council of Europe instruments are highly relevant. Firstly, the European Convention for the Protection of Human Rights and Fundamental Freedoms[22] (ECHR) particularly when it comes to the protection of the right to privacy. Secondly, the Council of Europe Convention on Mutual Assistance in Criminal Matters[23] and its 1978 Protocol.[24] This Convention entered into force on 12 June 1962 and has 50 States Parties, which includes all Member States of the EU. It does not have specific provisions on electronic evidence but is the widest measure of mutual assistance with a view to collecting evidence, hearing witnesses, experts and prosecuted persons, etc. in cross-border criminal cases. The Convention sets out rules for the enforcement of letters rogatory by the authorities of a State Party that aim to procure evidence or to communicate the evidence in criminal proceedings undertaken by the judicial authorities of another State Party and specifies the requirements for such proceedings. However, considering the year 1959 when it was adopted, the Convention on Mutual Assistance in Criminal Matters does not consider the modern technologies we are faced with today, making it a too slow a process for today's fast modern world. Finally, and most importantly, the third Council of Europe relevant instrument within the context of electronic evidence is the Council of Europe Convention on Cybercrime[25] (Cybercrime Convention). This Convention remains the main (and only) international treaty that defines the substantive elements that lead to some cyber activities to be classified as crimes and has procedural provisions that allow for the prevention, detection and prosecution of these activities. Although electronic evidence may not necessarily result from cybercrime, this is the main framework for reference in this area, which offers many provisions to enhance investigations where electronic evidence is involved.

The European Committee on Crime Problems (CDPC), which was set up in 1958 by the Council of Europe and is responsible for overseeing and coordinating

[21] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 9, 15; See also Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] OJ L 218, Recital 15.

[22] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] as amended by Protocols No. 11 and No. 14 [2010] CETS No. 194.

[23] European Convention on Mutual Assistance in Criminal Matters [1959] CETS 030.

[24] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters [1978] CETS 099.

[25] Convention on Cybercrime [2001] ETS 185.

the Council of Europe's activities in the field of crime prevention, decided in November 1996 to set up a committee of experts to deal with cybercrime because of the fast developments in technology. Following that decision, the Council's Committee of Ministers set up the Committee of Experts on Crime in Cyberspace (PC-CY), which started working on a draft international convention on cybercrime. The final draft of the Cybercrime Convention was approved by the CDPC in June 2001 and submitted to the Committee of Ministers for adoption and opening for signature.[26] The Cybercrime Convention was adopted on 8 November 2001 and opened for signature in Budapest on 23 November 2001. The Cybercrime Convention entered into force on the first of July 2004 and currently[27] has 53 ratifications and 4 signatures not yet followed by ratification (including few EU Member States[28]). The Cybercrime Convention goes beyond Europe as it includes several ratifications and signatories, which are non-members of the Council of Europe, such as the United States of America (USA), Japan and Australia.[29] The aim of the Cybercrime Convention is to harmonise domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime, to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as other offences committed by means of a computer system, or evidence in relation to which is in electronic form and to set up a fast and effective regime of international cooperation.[30] The investigative powers and procedures enshrined in the Cybercrime Convention also apply to the collection of evidence in electronic form of a criminal offence (Article 14 (2,c) Cybercrime Convention). Because of the very nature of cybercrime, the evidence in cybercrime cases is mostly in electronic form. Such evidence can easily be altered, meaning that the admissibility of the evidence may be at stake. Therefore, when collecting and handling electronic evidence, the integrity, authenticity and continuity of such evidence must be guaranteed during the entire chain of custody—from seizure until trial. Given the importance of electronic evidence particularly during the criminal process (in the prosecution of crimes), there is increasingly more attention to the setting of common standards for the acquisition, collection, custody and exchange of electronic evidence. While some states still apply traditional evidential rules to electronic evidence, some states already have special rules for electronic evidence.[31]

[26]Council of Europe, "Explanatory report to the Convention of Cybercrime" (ETS No 185), p. 1–4.

[27]Latest update: 20 March 2017.

[28]Ireland and Sweden have signed but not yet ratified the Cybercrime Convention.

[29]See also Deliverable 3.2 of the E-CRIME project (Grant Agreement Number 607775): E-CRIME Deliverable 3.2 final report on countermeasure including policy and enforcement responses, March 2015 for more information on cybercrimes and the Cybercrime Convention.

[30]Council of Europe, "Explanatory report to the Convention of Cybercrime" (ETS No 185), p. 4.

[31]United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 55. See more in Part II of this deliverable.

11.2.2.1 Investigative Powers

Effective investigation and prosecution is not possible without the proper powers for law enforcement. The Cybercrime Convention provides that the States Parties to the Convention shall adopt legislation and measures to establish powers and procedures for criminal investigations and proceedings to be applied to the offences referred to in the Convention, other criminal offences committed by means of a computer system and to the collection of electronic evidence (Article 14 of the Convention). These powers and procedures thus apply to electronic evidence in relation to any offence for law enforcement to secure electronic evidence. For investigations in criminal cases, law enforcement requires investigative powers to collect (electronic) evidence. In certain cases, traditional powers (interview, surveillance, etc.) might be sufficient, however, when it comes to electronic evidence, specific powers may be necessary to collect the evidence. Such powers may include search and seizure of stored computer data, real-time collection of traffic data and interception of content data considering that evidence may come in the form of computer files, logs, transmissions, metadata, computer data, etc. The Cybercrime Convention focusses on cybercrimes, but when it comes to handling electronic evidence the same techniques may be necessary and the same investigative powers may apply. However, there are big differences in national enforcement legislation and approach. In certain countries traditional investigative powers might be general enough to apply to cybercrime cases while in other countries traditional procedural laws might not cover cyber specific issues, making it necessary to have additional cyber specific legislation. In both cases legislation requires a clear scope of application of powers and sufficient legal authority for actions. According to the UN study, the main gaps in investigative powers include the lack of power to enter electronic networks to search for evidence and the lack of power to preserve computer data to support existing search powers. The same study also shows that Europe scores highest in the sufficiency of national law for cybercrime investigations, approximately 70% of responding European countries reported that investigative powers were sufficient. The remaining 30% responded that investigative powers were sufficient in part (25%) and not sufficient (5%). When investigating an (alleged) offence under the substantive law provision of the Cybercrime Convention, national law should at least provide some investigative powers including expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure, real-time collection of traffic data and interception of content data (Article 16–21 Cybercrime Convention). The Cybercrime Convention thus provides for powers for investigation and prosecution, which are specialised to investigations in an electronic environment, that can be highly intrusive. For this reason, the Convention stipulates that all investigative powers are subject to the conditions and safeguards under Article 15 of the Convention, meaning that they are to be executed with regard for human rights and the principle of proportionality.

11.2.2.2 Jurisdiction

When exercising investigative powers, particularly where electronic evidence is concerned, law enforcement may stumble upon evidence that is stored or located in another country so that jurisdiction may be problematic. For example, in cybercrime cases or when electronic evidence is stored in a cloud, the evidence may be located in another jurisdiction than the one investigating the crime. When it comes to cybercrime between 50 and 100% of cybercrime acts involve a transnational element.[32] Jurisdiction in such cases thus requires both executive and judicial jurisdiction to be effective.[33] Executive jurisdiction meaning the capacity of a state to act within the borders of another state and judicial jurisdiction meaning the power of a Court to try cases in which a foreign factor is present.[34] International law permits states to exercise jurisdiction on some principles.[35] The Cybercrime Convention relies on the territoriality and nationality principles to establish jurisdiction. According to Article 22 of the Cybercrime Convention, States Parties to the Convention are required to adopt legislative and other measures necessary to establish jurisdiction over the offences mentioned in the Cybercrime Convention when the offence is committed in its territory, on board a ship flying the flag of that Party, on board an aircraft registered under the laws of that Party or when the offence is committed by one of the nationals of a State Party, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

11.2.2.3 International Cooperation

If a state investigating a criminal offence does not have jurisdiction to collect evidence, which is stored or located in another country, international cooperation comes into play. Chapter 3 of the Cybercrime Convention regulates international cooperation. The chapter consists of two sections: general principles and specific provisions. The first section on general principles consists of general principles relating to international cooperation, principles related to extradition, general principles related to mutual assistance and procedures pertaining to mutual assistance requests in absence of applicable international agreements. In accordance with Article 23 of the Cybercrime Convention, the general principles relating to international cooperation, the States Parties to the Convention shall cooperate with each other, in accordance with the principles of the Convention, and through the application of relevant international instruments on international cooperation in

[32] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 55.

[33] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 55.

[34] See Shaw (2008), pp. 650, 651.

[35] See Shaw (2008), pp. 652–673. See also Brenner and Koops (2004).

criminal matters, arrangements agreed based on uniform or reciprocal legislation, and national laws, to the widest extent possible for investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. The principles based on which the Convention requires the States Parties to cooperate include extradition and mutual assistance. Apart from these principles, states may also be part of a broader network of multilateral and bilateral agreements relating to cooperation in criminal matters.

11.2.2.4 Mutual Assistance

Mutual assistance is the most important means of international cooperation and one of the most important aspects regulated by the Cybercrime Convention considering the cross-border nature of cybercrime. One of the main aims of mutual assistance is to obtain evidence for use in criminal proceedings and trials. Evidence collected abroad by the requested state and under its own procedures will need to meet the evidentiary rules of the requesting state. According to Article 25 (1) of the Cybercrime Convention States Parties to the Convention shall afford one another mutual assistance to the widest extent possible for investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Thus, mutual assistance is to be extensive and impediments strictly limited and is to be applied to both criminal offences related to computer systems and data and to the collection of electronic evidence of a criminal offence. The obligation to cooperate is thus a broad one, however, Article 34 and 35 permit States Parties to provide for a different scope of application of these measures. The obligation to provide mutual assistance is generally to be carried out pursuant to the terms of applicable mutual legal assistance treaties, laws and arrangements including bilateral or multilateral agreements. States Parties to the Convention are required to have a legal basis to carry out the specific forms of cooperation described in the remainder of the chapter, if its treaties, laws and arrangements do not already contain such provisions (Article 25 (2) Convention). The availability of such mechanisms, particularly those in Article 29–35, is vital for effective cooperation in computer related criminal matters. Mutual assistance typically requires lengthy verification of the validity of the request. In practice, this formal mutual assistance is often complemented by informal police-to-police or agency-to-agency communication in law enforcement investigations, which can be used prior to a formal mutual legal assistance request. In such informal communication the assistance of international LEAs such as Interpol or Europol may prove useful.

11.2.2.5 Gaps in the Investigative Framework

An effective enforcement scheme is required to have an effective international scheme for the collection, preservation and, in particular, exchange of electronic evidence. However, there are big differences in national enforcement legislation and approach and practices and readiness may vary significantly on the different levels of law enforcement (local, regional, national). Although international cooperation has proven successful, there are few realities that need to be faced as coordination is costly and difficult to carry out for trivial matters such as time zone differences and nuances of local laws and customs in the jurisdictions involved. One of the main challenges is the need for law enforcement to cooperate with third parties such as industry. Another main challenge is that technologies are developing rapidly and that policing technologies will need to be revolutionised with it. However, the UN cybercrime study shows that the capacities and resources of the police forces vary dramatically, especially at local level. The average police officer may lack the knowledge about new technologies and the average police unit may not have the right resources to handle electronic evidence. While some local police forces may have some sort of cyber unit, others barely have trained officers. Specifically, cybercrime offenders are highly equipped and skilled and enforcement cannot lag behind. This is especially important considering the growing importance of electronic evidence. Not all police forces are equipped to handle such evidence. It is therefore important to revolutionise policing technologies, capacities and knowledge. The critical elements of consistent and effective law enforcement should thus include an effective legal framework, access to investigative tools and techniques, training and technical capabilities and best practices policies that ensure proportionality between the protection of privacy and infringements for legitimate crime prevention and control.[36] The third main challenge is jurisdiction since electronic evidence may not consider national borders that leads to another main challenge when the investigating jurisdiction is required to ask for mutual assistance, which is a time-consuming procedure. The issue of when the investigating jurisdiction is permitted to unilaterally access computer data stored in another jurisdiction without seeking mutual assistance was a question that the drafters of the Cybercrime Convention discussed at length. Because of lack of experience and the understanding that it often depends on the circumstances of the case it was ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. Article 32 was the ultimate outcome. Thus, when faced with a cross-border case, law enforcers in most cases will have to ask for mutual assistance or pass on information to their counterparts across the border that is time consuming and, especially in the financial sector, often arrives too late. This has instigated an interesting discussion on hacking back or strikeback, meaning electronic countermeasures to track down hackers' computers and disable

[36] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 118.

them, which has been a growing sentiment in the financial sector. However, hacking back or striking back in itself is most likely an illegal act. These challenges in current legislation have not yet been addressed.[37]

One major criticism raised in literature (and by practitioners) is that the notion of territorial jurisdiction, particularly as the notion governing investigative powers is rather limiting and problematic in today's world where electronic information is processed, shared and stored across several territorial jurisdictions and spaces. What is being argued by Svantesson,[38] is that it is time to separate judicial and enforcement jurisdiction from investigative jurisdiction. While territorial scope of judicial and enforcement jurisdictions is logical and understandable; the territorial scope of investigative jurisdiction is unnecessarily limiting the access to cross-border data (and electronic evidence). The argument here is that in the case of an investigation, the investigative jurisdiction should extend to any space where the data required for the investigation is located.

While from a law enforcement access to cross-border data this development of 'investigative jurisdiction' may make sense in some cases, in others the current problems may still not be overcome. One scenario where the notion of 'investigative jurisdiction' may work is when a law enforcement agent is following a trail in real-time: the investigation should not stop because the suspect or suspected information shifts servers and is on a server outside the territorial reach of the law enforcement agent. Having an 'investigative jurisdiction' would allow the agent to follow the trail irrespective of territorial concerns. One scenario where this notion of 'investigative jurisdiction' may be less useful is when requiring information directly from a private actor: which rules would the private actor be expected to follow (of location or of the investigating party) is not immediately clear and would still be dependent on some form of legal agreement. Furthermore, as Svantsson notes "it should be acknowledged that some (coercive) investigate measures may fall within a grey zone between investigative jurisdiction and enforcement jurisdiction. This is an area requiring further work."[39] Within the EU, Council Framework Decision 2002/465/JHA regulates the setting up of JITs. To carry out criminal investigations in Member States, which necessitate coordinated and concerted action, at least two Member States may set up a JIT. To that end, the competent authorities of the

[37] See Guidance note adopted by T-CY on Article 32 issued in December 2014: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282013%297REV_GN3 _transborder_V12adopted.pdf; the work of the T-CY Cloud evidence group: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/Transborder%20Access/TCY_Transborder_EN.asp; Discussion paper prepared by the T-CY Cloud Evidence Group Criminal justice access to data in the cloud: challenges 2015 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf and Koops and Goodwin (2014).

[38] See Svantesson (2016) and Jerker et al. (2016), pp. 671–682.

[39] See Svantesson (2016), p. 8.

relevant Member States enter into an agreement determining the procedures to be followed by the team. The JIT must be set up for a specific purpose; and a limited period (which may be renewed with the agreement of all the parties involved). The Member States that set up the team decide on its composition, purpose and duration. They may also allow representatives of Europol and OLAF and representatives of third countries take part in the team's activities. Members of the JIT from Member States other than the Member State in which the team operates are referred to as being "seconded" to the team. They may carry out tasks in accordance with the law of the Member State where the team is operating. With respect to offences committed by them or against them, officials from a Member State other than the Member State of operation are to be regarded as officials of the Member State of operation.[40] Increasingly, this is being acknowledged as one of the most relevant instruments for LEAs to overcome territorial limitations in investigation of cross-border crimes and for sharing of cross-border electronic evidence.

11.2.3 Guidelines and Best Practices

Apart from the various existing international legal instruments there are also international guidelines and best practices, for example those provided by the EU and the Council of Europe that complement the legal instruments and provide practical guidance for handling electronic evidence. Given the importance of electronic evidence, particularly during the criminal process (in the prosecution of crimes), there is increasingly more attention to the setting of common standards for the acquisition, collection, custody and exchange of electronic evidence. While some states still apply traditional evidential rules to electronic evidence, some states already have special rules for electronic evidence.[41] Common standards include guidelines and best practices by the European Union Agency for Network and Information Security (ENISA) and by the Council of Europe. ENISA assists the EU and the Member States and cooperates with the private sector to help them meet the requirements of network and information security, it provides guidance, advice and assistance within its objectives.[42] To this end ENISA drafted a handbook[43] and a guide[44] to bridge the gap between Computer Emergency Response Teams (CERTs)—teams responsible for handling cyber incidents and risks—and law enforcement. According to ENISA

[40] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33172.

[41] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 55.

[42] Article 1 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77.

[43] ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013.

[44] ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014].

effective cooperation on all levels is required when it comes to cyber incidents as they do not respect organisational and territorial boundaries. While collecting and preserving electronic evidence is ultimately a task and responsibility of law enforcement, CERTs may aid law enforcement in preserving it when they detect an incident.[45] ENISA's electronic evidence guide provides guidance for CERTs on how to deal with evidence and evidence collection. According to this guide there are five internationally accepted practical principles that are considered a good basic guideline; data integrity, audit trail, specialist support, appropriate training and legality.[46] The handbook divides the collection of electronic evidence in few phases, namely: preparation, on-site, seizure, examination, evaluation and presentation.[47] The ENISA handbook and guide lack information regarding the exchange of electronic evidence. It focusses mainly on collecting evidence and a little bit on preserving and presenting (using) the evidence. It furthermore does not mention anything regarding data protection or secure systems used to exchange the data. Furthermore, from discussions with LEAs, it appears that they often consider the ENISA guidelines as more tailored towards private companies rather than LEAs. Another set of common standards is provided by the Council of Europe. The Council of Europe developed the Electronic Evidence Guide[48] (EEG) intended for use by law enforcement and judicial authorities.[49] The purpose of the guide is to provide support and guidance in the identification and handling of electronic evidence, i.e. developing responses to cybercrime and establishing rules and protocols to deal with electronic evidence. The guide may particularly be useful for training and self-training as it was developed for a wider audience including law enforcement, judges, prosecutors, private investigators, lawyers, notaries, etc. The EEG identifies the possible sources of electronic evidence and uses the same principles, as a basis that

[45]ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014], p. iv.

[46]ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014], p. 5–8. These principles are discussed in more detail in the handbook: ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013. The principles used by ENISA are the same principles used by the Council of Europe in its Electronic Evidence Guide: Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available via: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

[47]ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014], p. 9–19. See also ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013.

[48]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges version 1.0, Strasbourg, France, 18 March 2013.

[49]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp.

justifies all dealings with electronic evidence, as the ENISA handbook and guide (data integrity, audit trail, specialist support, appropriate training, legality).[50] When it comes to the collection of electronic evidence the EEG provides detailed guidance on how to search and seize onsite, how to capture evidence from the internet and how to collect evidence from third parties. The EEG furthermore provides guidance on the analysis of electronic evidence and how to prepare and present (use) the evidence in Court. Considering the complexity of cross-border crimes and dealing with electronic evidence the EEG furthermore devotes a chapter on jurisdiction and roles of the various actors. The EEG does not go into detail on the exchange of electronic evidence, but refers to the mutual legal assistance provisions in the Cybercrime Convention.[51]

11.2.4 Actors

As pointed out in chapter *The Operational Scenario* of this Volume, on a national level the actors involved in the collection, preservation, use and exchange of electronic evidence include law enforcement authorities including police forces on local, regional and national level, cybercrime units and specialised forces, prosecution and the judiciary. There are thus a massive number of actors involved. These national authorities are supported by various international and European agencies and bodies that assist Member States in preventing, detecting, investigating and prosecuting cross-border crimes. This is highly relevant when it comes to electronic evidence as these agencies and bodies may assist in international cooperation, collection and facilitate the exchange of electronic evidence. These authorities include Interpol and various EU agencies and bodies, such as Eurojust, Europol (EC3) and ENISA.

Interpol is an organisation under international law and the world's largest international police organisation with 192-member countries, which enables police around the world to work together. Interpol is a global coordinating body that ensures and promotes the widest possible mutual assistance between all criminal police authorities and establishes and develops institutions likely to contribute

[50]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available via: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp, p. 14–15. See also ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014], p. 5–8; ENISA, Identification and handling of electronic evidence—Handbook, document for teachers [2013] September 2013.

[51]Council of Europe Data Protection and Cybercrime Division, Electronic Evidence Guide A basic guide for police officers, prosecutors and judges Version 1.0, Strasbourg France 18 March 2013, available via: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp, p. 14–15. See also ENISA, Electronic evidence—a basic guide for First Responders Good practice material for CERT first responders [2014], p. 152.

effectively to the prevention and suppression of crimes.[52] This global coordination pays off. Operations coordinated by Interpol, Europol and/or Ameripol[53] with the support of LEAs from all over the globe has led to numerous arrests in multiple jurisdictions.[54] Interpol has a high-tech infrastructure of technical and operational support and ensures that police around the world have access to the tools and services necessary to do their jobs effectively. Interpol furthermore provides targeted training, expert investigative support, relevant data and secure communications channels and facilitates international police cooperation. Concerning cybercrime, Interpol has a new cutting-edge research and development facility, the Global Complex for Innovation (IGCI) that includes a Digital Crime Centre. This centre provides proactive research into new areas and latest training techniques, and coordinates operations in the field. The initiative about cybercrime focusses mainly on harmonisation (encouraging the creation of cybercrime investigation units and updating legal frameworks), capacity building (training courses) and operational and forensic support (Cyber Fusion Centre providing assistance during investigations, Digital Forensics lab providing practical forensic support and Working Groups Working Groups facilitating the development of regional strategies, technologies and information on the latest crime trends and methods).[55]

Interpol's European counterpart is the European Police Office (Europol), which is the EU's law enforcement agency whose main goal is to help achieve a safer Europe for the benefit of all EU citizens by assisting Member States in their fight against serious international crime and terrorism. The establishment of Europol was agreed in the Maastricht Treaty[56] and regulated in the Europol Convention,[57] which was replaced in 2010 by Council Decision 2009/371/JHA[58] and in 2016 by the Europol Regulation.[59] The new Regulation extends Europol's role and responsibilities in coordinating crime investigations and constitutes the legal basis of a new framework for Europol including a new opt-in decision that is required by Member States. This Regulation particularly names the development of the European Cybercrime Centre (EC3) as one of its key objectives. Europol supports and strengthens action by the competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious

[52]Interpol Office of legal affairs, Constitution of the ICPO-INTERPOL, I/CONS/GA/1956(2008).

[53]The Police community of the Americas.

[54]See: <http://www.interpol.int/News-and-media/News>.

[55]See: http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

[56]Treaty on European Union of 7 February 1992.

[57]Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office [1995] OJ C 316/2.

[58]Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA) [2009] OJ L 121/37.

[59]Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and Replacing and Repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] OJ L 135/53.

crime. Europol staff may furthermore participate in supporting capacity in JITs. Europol's tasks include, amongst other things, to collect, store, process, analyse and exchange information and intelligence and to aid investigations in the Member States and developing specialist knowledge of investigative procedures. Each Member State has a Europol national unit, which is the liaison body between Europol and the competent authorities of the Member States. Each national unit has at least one liaison officer at the Europol headquarters in their own liaison bureau as part of the organisation mentioned before. These officers represent the interests of their national unit at Europol in accordance with the national law of their Member State. Apart from the liaison officers of the Member States Europol also hosts liaison officers from 10 non-EU countries and organisations that work together with Europol based on cooperation agreements including Interpol and several USA LEAs. In return Europol also has liaison officers in Washington DC and Interpol. This network is supported by secure channels of communication provided by Europol. Europol does not have an explicit mandate to handle electronic evidence. However, Europol's secure system "Siena" is frequently used to transfer documents. These documents may come from a competent authority in a Member State and may be sent from the national unit in that Member State to Europol and via Europol to one or more national units in other Member States, which in its turn send it to the competent authorities. The Sienna system is used between all the members of the network mentioned before. This means that the transfer from the national units to the competent authorities in the Member States need to be secured by the Member States and that the Sienna system does not provide security from end point to end point. This might provide security problems. With specific regard to cybercrime Europol has a European Cybercrime Centre (EC3) and a Joint Cybercrime Action Taskforce (J-CAT). EC3 is part of the operations department and its main task includes providing support to Member States concerning cybercrime. J-CAT further strengthens the fight against cybercrime in the EU and beyond.[60] J-CAT is a pilot hosted at the EC3 that coordinates international investigations with partners from all over the world including the UK's National Crime Agency (NCA), EC3, Eurojust, EU Cybercrime Taskforce, the Federal Bureau of Investigation (FBI) and other USA agencies NCA's with cyber liaison officers from countries including Austria, Canada, Germany, France, Italy, the Netherlands, Spain, the UK, etc. J-CAT already booked some successes, for example in taking down dark markets on the TOR network.[61]

Apart from Europol, the EU also set up Eurojust, a unit composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to their own legal systems. Eurojust was formally established as a judicial coordination unit in 2002 by Council Decision

[60] See: https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime.

[61] See: https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network.

2002/187/JHA[62] following the 9/11 attacks in the USA. The Decision was amended in 2003 by Council Decision 2003/659/JHA and in 2008 by Council Decision 2009/426/JHA. A consolidated version of the Decisions was published in 2009.[63] Eurojust is composed of 28 national members seconded by each Member State in accordance with its legal system, who is a prosecutor, judge or police officer of equivalent competence. The national officers have their regular place of work at the Eurojust seat in The Hague and are assisted by a deputy and an assistant. The national members, deputies and assistants are subject to the national law of their Member State regarding their status.[64] All 28 national members form the College of Eurojust, which is responsible for the organisation and operation of Eurojust. The College of Eurojust is supported by an administration and secretariat and is supervised by an independent joint supervisory body and a data protection office. Eurojust assists the competent authorities of Member States when dealing with cross border criminal matters. It stimulates and improves cooperation and coordination of investigations and prosecutions between the competent authorities in Member States, particularly organised crimes and crimes and offences in respect of which Europol is competent.[65] It does so for example by facilitating the execution of international mutual legal assistance and the implementation of extradition requests. It supports the competent authorities to make their investigations and prosecutions more effective in cross border cases and may, at the request of a Member State, assist in investigations and prosecutions concerning that particular Member State and a non-Member State if a cooperation agreement has been concluded or if an essential interest in providing such assistance is demonstrated.[66] Eurojust has a facilitating role in the sense that it makes requests rather than give orders, it provides advice (for example regarding jurisdiction), builds relationships with different stakeholders across Europe and hosts coordination meetings (for example when search and seizure on multiple locations in Europe take place on the same day). The competent authorities and Eurojust exchange any information necessary for the performance of its objectives and tasks.[67] Although not explicitly mentioned as such, this may include electronic evidence. Based on the Decision data security is provided for. Eurojust uses a system to communicate with home authorities that is fit for purpose.

[62]Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA) [2002] OJ L 63/1.

[63]Council of the European Union, Consolidated version of Council decisions 2002/187/JHA, 2003/659/JHA and 2009/426/JHA, Brussels 15 July 2009, 5347/3/09 REV 3.

[64]Article 2 Council of the European Union, Consolidated version of Council decisions 2002/187/JHA, 2003/659/JHA and 2009/426/JHA, Brussels 15 July 2009, 5347/3/09 REV 3.

[65]Article 3 and 4 Council of the European Union, Consolidated version of Council decisions 2002/187/JHA, 2003/659/JHA and 2009/426/JHA, Brussels 15 July 2009, 5347/3/09 REV 3.

[66]See: http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx.

[67]Article 13 and 13a Council of the European Union, Consolidated version of Council decisions 2002/187/JHA, 2003/659/JHA and 2009/426/JHA, Brussels 15 July 2009, 5347/3/09 REV 3.

11.3 National Legislation and Practices

While the use of new technologies in the commission of old and new crimes (cybercrimes), contribute to make the collection and exchange of electronic evidence increasingly relevant in criminal justice, this evolution and gradual digitisation of the means necessary to collect and analyse electronic evidence has not been accompanied by a consistent and uniform evolution of the legal frameworks across Europe. Different rules and practices regarding the collection, preservation, use and exchange of electronic evidence exist in the European countries. Given the increasing use of digital devices in daily activities the attention for electronic evidence in the European and national legislation is expected to increase. While there is a certain amount of EU competence to harmonise some aspects of criminal procedural laws and to facilitate cooperation among states (e.g. providing minimum rules on mutual recognition of judgements and judicial cooperation), the competence to legislate in the field of criminal matters was left to the Member States. Most criminal laws in the European countries have a long historical background and were written long before the digital age. Legal traditions and approach thus vary per country, even per countries with similar legal traditions. Moreover, electronic evidence particularly is hardly regulated at all and a specific legal definition of electronic evidence does not exist in the European countries. The common trend among the legal frameworks is to apply general principles and rules regarding traditional evidence (on collection, exchange and probative value) also to cases involving electronic evidence. In the last years there was a slow but gradual interpretative evolution of the national criminal laws regarding the treatment of evidence, which allowed the competent actors (judges, prosecutors, lawyers, LEAs) to apply, to some extent, existing norms to cases involving electronic evidence. In other cases, some amendments to existing norms of criminal law (substantial and procedural) were necessary to make them applicable to the new technological scenarios and yet in other cases, the amendments have been considerable, comprising the replacement of, for instance, entire articles or even sections of the national criminal procedural law or the introduction of new articles also because of the implementation of a supranational legislation (e.g. the Cybercrime Convention). These laws and regulation need to be applied and interpreted accordingly by the actors involved. Although the specific knowledge and expertise of the main actors involved in the handling of electronic evidence seems to increase and best practices are gradually developing, there is, in general, a lack of knowledge by some of the main actors, as well as a lack of specific standards on the procedures and modalities to follow in the phase of collection, preservation and especially in the exchange of electronic evidence. Even when best practices do exist, they are rarely mentioned in the national laws but more often contained in non-binding texts.

The EVIDENCE project researched the need for legislative measures at the European level and created a roadmap for a uniform and efficient application of digital technologies in the collection, use and exchange of evidence. To be able to assess the need for legislative measures at European level it was necessary to research the

status quo of the European legal frameworks covering the electronic evidence and to offer a picture of the existing laws and practices related to the electronic evidence. An in-depth study of thirteen EU Member States,[68] representative of different legal traditions and areas of Europe and a high level overview of the remaining Member States was carried out. The remainder of this chapter offers an extract of the results of the research carried out in this regard.

11.3.1 Differences and Similarities Between Member States

Differences in the national legal systems or the system of protection of fundamental rights may have an impact on the practices governing the handling of electronic evidence. This may have an impact on, for example, admissibility in Court in cross-border cases. To collect electronic evidence, different measures can be taken. Some Member States for example make a distinction between preventive and investigative or repressive measures. Preventive measures (including collecting electronic information, such as preventive interception of communications) are aimed at impeding, preventing the commission of crimes and at ensuring the public order in situations or in relation to individuals deemed by the competent authorities to be dangerous for society. Preventative measures are in general a competence of national bodies dependent on the Ministry of Interior and may be adopted by LEAs, police and other bodies competent to safeguard national security and may also fall within the general competences of national Security and Intelligence Services (SIS). Investigative or repressive measures are usually a competence of LEAs and police forces and presuppose the commission of a fact that might be deemed as a crime and therefore, they are aimed at investigating and collecting information on committed crimes. Transfer of information or actionable intelligence between SIS and LEAs and vice-versa is often not regulated. The distinction in legal treatment (and application of laws) to LEAs and SIS is not always clear. In most cases, the prime function of SIS is to produce actionable intelligence, which is passed on to the LEAs to act, whether it is to further monitor, follow, detain, arrest or prosecute a person or group of persons. However, there is a general lack of rules in the transfer and exchange of information or actionable intelligence and whether this information can be admitted as evidence in a criminal trial. Rules in this regard are necessary to establish whether the information or actionable intelligence can be admitted as evidence in a criminal trial. If the origin of the data is unknown or if the data was collected by SIS, the legitimacy of the source and transfer might be put in question as a clear chain of custody and documentation thereof is missing. In countries where a clear distinction between preventive and investigative measures exists the information collected for preventive purposes usually could generally not be legally used afterwards as evidence in Court. Data collected in the context of a preventive measure can however often be used as a

[68]Belgium, Bulgaria, Croatia, Denmark, Finland, Germany, Hungary, Italy, The Netherlands, Poland, Spain, Sweden and The United Kingdom.

starting point for an investigation. The functional distinction between preventive and investigative measures does not necessarily correspond to a distinction of the actors involved, i.e. both type of measures may well fall within the competence of several authorities, who may act sometimes for preventive and other times for investigative purposes and in collaboration with each other.[69] Preventive measures, such as covert surveillance on communications aimed at acquiring information necessary to ensure national public security, may be executed by SIS that generally do not have executive powers (such as arrest, search or seizure of data). These powers are exercised by LEAs and police forces based on the information transmitted by SIS.[70] These powers need to be executed regarding privacy, data protection and related rights within the system of fundamental rights. Where specific safeguards apply for the protection of fundamental rights, this may have an impact on the lawfulness and consequences of investigative measures aimed at collecting, preserving or exchanging electronic evidence. There are slight differences between Member States regarding whether and how the national legal systems provide for fundamental rights, such as data protection, telecommunications privacy, integrity of IT systems or other fundamental rights that can be affected by the collection and use of electronic evidence. Beside the different historical-cultural conceptions of these rights and the constitutional traditions of the Member States, this varied landscape is attributable to the slightly different implementation of related European legislation (e.g. in the field of data protection) and to the interpretation of these rights by the Courts of each country, particularly as it comes to deciding limits and safeguards in relation to other national rules, such as rules of criminal justice that are traditionally a competence of national Member States.[71]

11.3.1.1 Applicable Law

All legal frameworks require a legal basis for the adoption of investigative measures, such as search and seizure and any other measures in the collection, preservation, use and exchange of electronic evidence. As a general consideration it can be said that national law(s) in evidence and criminal proceedings have hardly been adjusted

[69] Italy for example has different forces, including Polizia, Guardia di Finanza and Carabinieri.

[70] In Italy and Germany for example, SIS are entitled only to gather information conducting researches and coordinating activities; this can happen through measures technically similar to those taken by the police (e.g. wire-tapping), although the adoption of these measures need to be laid down in distinct provisions defining the related conditions and purposes. From the gathered intelligence, the services can notify the police where appropriate. In northern countries such as Sweden, Finland, Denmark and Poland this distinction does not have so much relevance or it is not well-defined.

[71] Moreover, concerning the Members States' obligations on human rights as derived by international treaties, it should be recalled here that, for instance, in the application of the European Convention of Human Rights (that includes the right to privacy and other fundamental rights), the ratifying States gain a *margin of appreciation* on *how* to ensure certain rights enshrined in the Convention.

to the increasing use of new technologies, as well as on the limitations they provide in electronic evidence, including in case of collection of data by or through third parties, such as Internet Service Providers (ISPs). With a few exceptions, Member States in general do not have separate, specific rules in electronic evidence and apply general, traditional evidence rules to electronic evidence. It is striking that, with the exception of Croatia,[72] none of the Member States, which were considered for the EVIDENCE project, provides for a definition of electronic evidence. The general trend is to apply a general definition of evidence, as well as general principles of evidence also to electronic evidence. Having said that, the common factor of all Member States is that they have ratified the Cybercrime Convention and have thus introduced some rules applicable to electronic evidence into their legal frameworks. National legal frameworks applicable to electronic evidence are quite limited and fragmented, but it is possible to identify substantial and procedural norms in national legislation that are, subject to judicial interpretation, applicable to the cases that involve electronic evidence. Moreover, in some countries, specific norms have been introduced to criminal law and criminal procedural law to adapt the legal framework to the growing use of digital technologies which distinguish between physical and electronic evidence and which provide indications concerning the procedure to be followed for collecting, preserving and lawfully exchanging electronic evidence. Most of these changes to the national legal frameworks have been introduced as implementation of supranational treaties, such as the Cybercrime Convention or European legislation in related fields.

Considering that Member States in general do not have specific rules in electronic evidence the question arises whether national legislations pose any restrictions to the collection, use and admissibility of electronic evidence in Court. The answer to this question becomes clear only in 'digital documents', which are generally considered admissible in Courts and used in practice, although the conditions for their admissibility may vary according to the legal system. Some guidelines exist, although these are mainly aimed at preserving the security of (electronic) evidence during and after the trial, such as for example in England and Wales. Methods and systems to preserve (electronic) evidence vary per country and it is striking that in this digital age the digital filing systems used are often still limited in that they are generally non-interoperable systems and for internal use only. However, some countries have a more advanced digitalisation of documents where digital filing systems are used also for the exchange of data between authorities or files sent to Court electronically. For example, in Poland digitalisation of documents is encouraged and the digital filing systems are used also for the exchange of data between authorities and in Sweden the file (dossier or book of evidence) is sent to the Court electronically when charges are brought against an individual. In many cases however, digital documents are still printed out and deposited at the Courts on a physical carrier. It is furthermore striking that there is a general lack of standards

[72]Croatian Law CPC Article 202 (32) determines that *electronic (digital) evidence means data that was collected as evidence in the electronic (digital) form pursuant to this Act*.

or uniform application of digital technologies in collecting, preserving, using and exchanging evidence. Beside the existence of ISO international standards, most Member States use non-binding guidelines or procedures that include technical procedures such as chain of custody or specific forensic-technical norms. Among the conditions and procedural requirements established by law for the collection, preservation, use and exchange of electronic evidence, mention should be made of those requirements aimed at safeguarding individuals against violation of data protection rights, as well as against 'function creep', i.e. e-evidence collected for a certain purpose may end up being used for a different purpose. In this respect, the concept of 'surplus information' that can be found for example in Finland and Denmark is very interesting. Surplus information is information obtained by telecommunications interception, traffic data monitoring, obtaining base station data and technical surveillance that is not related to an offence or averting a danger, or that concerns an offence other than the one for the prevention of which the authorisation has been granted or the decision made. Only in some countries can the evidence collected for a certain case be used in different proceedings under specific safeguards.

11.3.1.2 New Technologies and Investigative Measures

In this digital age where technologies keep evolving, so do crimes. Criminals may use advanced technologies and law enforcement cannot lag behind. New technologies have influenced the different techniques of investigation that law enforcement and prosecution use in criminal proceedings. Most legal frameworks include rules covering the legal and technical procedures that need to be followed in the collection of electronic evidence in criminal investigations. These procedures primarily aim at ensuring a minimum set of legal safeguards (e.g. judicial oversight) and, secondly, at ensuring the integrity, reliability and preservation of the evidence itself. However, these existing rules remain quite general and imprecise for the technical measures to be adopted. As general rules regarding the collection of traditional evidence (e.g. inspection and seizure) usually apply, the evidence is considered admissible in Court if it has been collected in accordance with the law. Its probative value is usually deemed to be the same as of the traditional evidence, although the (level of) authenticity and reliability of the electronic evidence may play a relevant role on this regard. There is a general consensus regarding the effectiveness of using digital technologies in the collection of evidence; technologies make copying and transferring data easier and facilitates exchange, it enables investigative bodies to collect a much wider spectrum of information, improves the speed and accuracy of investigation as it allows access to information about a suspect's activities for a long period, it ensures the collection of sturdy and precise information about a committed crime, allows the collection of evidence that was previously unavailable and safeguards the integrity, reliability and preservation of electronic evidence.

11.3.1.3 Lawful Interception

Electronic evidence can be collected in different ways, including by way of lawful interception. Within the legal frameworks across Europe the following interceptions are distinguished:

- Lawful interception of digital data in a network (e.g. internet);
- Direct access to a terminal device;
- Computer assisted search and;
- Seizure of digital data.

While in some countries certain specific provisions have been introduced in the national criminal system to cover at least some of the new kinds of interceptions of digital communications, in other countries these provisions do not exist and general rules on interceptions may apply. The common trend is that, in general, interceptions are considered exceptional, admitted only in relation to serious crimes (although the definition of serious crimes varies per country) and are subject to legal procedures (e.g. judicial warrant). However, it is not always clear what legal regime would apply in case of interceptions of digital devices by certain modalities, such as covert monitoring of computer devices, as in some countries this would fall within the special investigative measures, permitted only under 'national security' investigations. This means that the legal safeguards that these legal procedures seek to ensure may be jeopardised by the absence of a clear legal framework that is worrisome considering the development of digital technologies and the ease for LEAs and SIS to access large amounts of data, especially on the internet. In this regard it is also important to mention that, because of the Court of Justice of the European Union (CJEU) ruling which invalidated the Data Retention Directive,[73] some national legal frameworks across Europe were subject to constitutional review before the respective Constitutional Courts and declared unconstitutional. For example, Germany invalidated its national Data Retention law as unconstitutional and does not require ISPs and telecom companies to retain their clients' traffic data while other countries do. In other countries the corresponding law is still in force or new legislation was put in place.[74] These issues are further developed and discussed in Chap. 13 of this Volume.

11.3.1.4 Preservation and Use

Electronic evidence is volatile, it can be quite easily altered or deleted. It is therefore very important to have rules in place regarding chain of custody, preservation

[73]CJEU, C-293/12 Digital Rights Ireland, ECLI: EU: C104:238.

[74]In CJEU, C-203-15 Tele2 Sverige, ECLI:EU:C2016:970 the CJEU also held that national laws providing for the retention of traffic data need to be in line with Article 7 and 8 of the Charter of Fundamental Rights of the European Union.

and access control. Most legal frameworks do not determine explicitly who is authorised to process electronic evidence. Processing electronic evidence, particularly search and seizure of computer data and information systems, requires expertise and knowledge. In general, national Courts appoint a consultant or judicial expert to process the evidence. However, there is a general lack of binding rules regarding professional requirements. With a few exceptions where norms have been introduced, to consider preservation of seized computer data and information systems, in most cases general rules of preservation of evidence also applies to electronic evidence. Where norms have been introduced, these are binding only in the results ('suitable measures to preserve the authenticity, integrity and reliability of data'), not in technical methods to be adopted. Generally, operating procedures for the preservation of electronic evidence exist in secondary legislation or internal rules. Increasingly, electronic evidence nowadays is held by the private sector. In this regard there is a general lack of rules and procedures for LEAs to comply with when accessing data held by the private sector. In general, LEAs need to obtain authorisation by a Court to access this data. There is a consensus that digital technologies make processing and preserving evidence more effective. Digital technologies can offer advantages when handling large amounts of data. Considering that electronic evidence can be copied, a larger amount of people and even several competent authorities can work simultaneously on the same case to investigate the large amount of data. Preserving electronic evidence furthermore does not require much physical space compared to physical evidence and it is easier and more cost efficient to preserve electronic evidence over a longer timeframe while protecting its integrity, reliability and keep it from being altered. However, this requires secure storage. From a prosecution perspective, the use of computers and electronically accessible files by prosecutors during trial opens possibilities for the use of more pedagogical methods to explain a complex case in a way that gives full effect to the value of the evidence. However, as much as technology aids to acquire and process large amounts of data, if the evidence is preserved for long amount of time, from a technical perspective, the hardware and/or software used may become obsolete and the authenticity and trustworthiness of the electronic evidence could be put in question. Records or electronic evidence management systems should be build, organised and preserved by trained professionals in modern archival procedures of digital preservation.

11.3.1.5 Admissibility and Probative Value

The evidence collected in criminal investigations will eventually need to be used in Court. In cross-border cases, when the evidence was collected under the rules of a different legal regime, the question rises whether the evidence is admissible in Court. While some countries have specific best practices and practical guidelines (including technical procedures) that are used in practice in the collection,

preservation and exchange of electronic evidence,[75] others countries do not have any publicly available information on operational guidelines or on specific codes of conduct. Technical or automated means, which are possibly used by LEAs in investigations, are defined broadly. The only explicit legal limitation to the use of digital technologies in the collection, preservation and exchange that may affect the admissibility of electronic evidence are those arising from general rules on the collection of evidence. This includes rules that require the evidence to be collected in respect of certain procedural requirements and in a lawful manner, i.e. legal safeguards to avoid breach of fundamental rights.[76] Courts will generally decide on admissibility of evidence on a case by case basis and if the evidence is collected contrary to legal safeguards it may be declared inadmissible. For instance, the issue of admissibility may arise when evidence is illegally obtained because the conditions for applying the measures that led to the collection of evidence were not fulfilled. However, since these measures are in general under the control of the Court, in most of the cases admissibility issues are avoided. As for the probative value of electronic evidence, rules that count are usually those aimed at ensuring the authenticity, integrity and reliability of the evidence (e.g. irregularities may affect the trustworthiness of evidence).[77] In practice, although the national legal systems do not have explicit regulations on the probative value of electronic evidence and no standards exist, it is generally recognised as very important to duly document the data acquisition procedure, for instance, the interception techniques used and how the evidence has been preserved, according to the chain of custody. Therefore, the electronic nature of evidence, while it does not seem to affect its admissibility, it may have impact on its probative value (quality), depending on the evidence and how it was obtained. The problem seems to be more 'how' to interpret the conclusions that one can draw from the (forensic) findings resulting from a digital evidence. For those reasons, in most of the countries, Courts refer to (forensic) experts to examine the electronic evidence (including the procedure used in individual cases to collect it) and to provide their assessment and evaluation. Forensic experts seem to play an important role as expert witnesses, to explain and thereby give reliability to the electronic evidence. Therefore, judges usually base their decision on experts' analysis, although they remain free to decide differently, if they motivate their judgements. This also means that it is essential that the judge can truly understand how the evidence has been handled and is able to determine its authenticity. However, the level of knowledge of the judiciary still lags behind

[75] See Mason (2012).

[76] See e.g., rules safeguarding the right to due process or fundamental right, including, in certain cases, data protection: the compliance with the latter, although cannot be considered as general 'conditio sine qua non' for the admissibility of electronic evidence, may affect the admissibility of evidence in certain countries.

[77] For instance in Germany, the general legal conditions of §9 BDSG obliges law enforcement agencies as public authorities to secure their systems and digital technology-based investigative measures through technical and organisational measures.

dramatically considering that there is a general lack of training and education in this regard.

11.3.1.6 Cross-Border Scenarios

Considering that electronic evidence is not necessarily linked to the same territorial jurisdiction as where an alleged crime would have taken place or is being investigated, cross-border scenarios are an important aspect when dealing with electronic evidence. There are three aspects of this cross-border nature of electronic evidence: (1) where the evidence may be located because of the information provider recording the information[78]; (2) where the actual digital information is stored[79]; and (3) where the crime itself has a cross-border nature.[80] These three effects of the cross-border nature of electronic evidence are very important when regulating electronic evidence in the criminal law process. Cross-border scenarios and exchanging electronic evidence between the competent authorities of the countries involved are thus an important part of legislation in electronic evidence considering the very nature of electronic evidence and that it can be stored or located globally. However, current national and international legal frameworks are insufficient to meet with the current needs and current shortcomings are not merely a matter of introducing new agreements but are more complex, needing new theoretical frameworks and the collaboration of a large variety of actors. As mentioned before, the Cybercrime Convention (as well as the other international and European legal instruments) is the common factor between Member States and the leading legal instrument in Europe and beyond to exchange electronic evidence. International laws are implemented in the national legal systems of Member States and impact on investigations of national prosecution authorities that exceed national borders. Most Member States have national legislation covering cases of requests for exchange of evidence in general or exchange evidence pursuant to bilateral or multilateral agreements (e.g. European Convention on Mutual Assistance in Criminal Matters). Legislation mostly refers to evidence in general and does not specifically mention electronic evidence. In cross-border scenarios, cloud services

[78] *Location of (private) information provider*: Many forms of electronic evidence originates from private sources e.g. internet services providers have access/possess useful electronic information that can at times be used as electronic evidence in a trial. Many of the key private actors involved are not registered or located in the same country where a particular crime is being investigated and prosecuted.

[79] *Location and storage of electronic evidence*: Because of the very nature of it, modern technologies and growing globalisation, electronic evidence may be located or stored anywhere in the world. This is especially the case in cybercrime cases, as cybercrime is a global problem that does not stop at our countries' borders, but also increasingly in crimes in general.

[80] *Cross-border nature of the alleged crime*: In some crimes e.g. cybercrimes, the crime often takes place across different jurisdictions, making the collection, preservation and use of information for evidentiary purposes more difficult and reliant on pre-existing agreements between states (where these exist) for the exchange of electronic evidence.

for data storage have become an increasingly interesting area that is hardly covered by legislation. Legally speaking, this cloud services are particularly interesting considering that the cloud service provider, the data centres and the 'suspect' may be located in different countries. Various legal challenges pop up in this regard, including investigative issues and questions of jurisdiction. This is a relatively new area, meaning that the academic and public debate on these issues are still ongoing and that there is hardly any research in this field, let alone legislation covering the collection or exchange of electronic evidence that is stored in the cloud. Considering that there is hardly any specific legislation covering this topic, the Cybercrime Convention and general evidentiary rules on evidence apply and are left to the discretion of the national judicial authorities. For example, in cases where the cloud service provider or the suspect are located in a known foreign country, the general rules for the collection of other evidences apply. In cases where the physical storage location is unknown, the legal scenario becomes more problematic. This impacts investigation of evidence located in cloud services. Considering the very nature of electronic evidence and that it can be stored or located anywhere in the world, the exchange of electronic evidence between competent authorities in cross-border scenarios is a very important aspect when dealing with electronic evidence. While there is international legislation in this regard as elaborated in the first part of this chapter, there is a general lack of regulation in national legislation concerning the exchange of electronic evidence. Member States hardly provide for specific rules, guidelines or procedures on the exchange of electronic evidence and apply general rules and guidelines that are applicable to traditional evidence.

What national laws seem to ignore is the overwhelmingly cross-border nature of electronic evidence. The presence of electronic evidence is often not linked to the same territorial jurisdiction as where an alleged crime would have taken place or is being investigated. Given that predominantly territorial nature of judicial (or adjudicative) and enforcement jurisdiction of most crimes, any cross-border element to a crime or evidence of a crime is primarily regulated through international agreements concluded for this purpose between states. The same applies to the cross-border nature of electronic evidence. However, there is no comprehensive international or European legal framework relating to (electronic) evidence. What is present is a patchwork of international and European legal instruments and policy documents as mentioned before, as well as bilateral and multilateral agreements, which govern some of the issues often in an unsatisfactory manner. For example, when obtaining (electronic) evidence from a different country, within the EU, the EIO Directive[81] sets up a comprehensive new system that allows EU Member States to obtain evidence in other Member States in criminal cases that involve more than one Member State. The EIO covers any investigative measure except for the setting up of a JIT and the collection of evidence within such a team as provided in Article 13 of the Convention on Mutual Assistance in Criminal Matters. Within

[81]Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L 130/1.

all of Europe, the Council of Europe Convention on Mutual Assistance in Criminal Matters also applies which sets out rules for the enforcement of letters rogatory by the authorities of a Party that aim to procure evidence or to communicate the evidence in criminal proceedings undertaken by the judicial authorities of another Party and specifies the requirements for such proceedings. These general rules and guidelines were of course introduced with traditional evidence in mind. Most states have extended their application also to electronic evidence. While this is the most used method to obtain evidence from other countries, the process is slow, bureaucratic and time consuming and does not match the volatile and fast-moving nature of electronic evidence.

Perhaps the strongest drawback is that it is primarily aimed at states and not private actors considering that in many instances electronic information is under the control of private actors such as the larger ISPs, including Google, Facebook, Yahoo, etc. From yearly disclosure reports of some of these companies[82] several hundreds of thousands of requests for information go out every year from European states to major USA providers. Each of these requests need to be accompanied by a mutual legal assistance request for the information to be considered admissible as evidence by the courts of the requesting state. These mutual legal assistance requests go from the requesting state authority to the requested state then the requested state must transmit that request (subject to few legal requirements) to the private company. It is important to keep in mind that this cumbersome process needs to be followed for evidence that may be easily deleted, moved or changed to another format (e.g. encrypted) and where speed of capture or seizing the evidence is crucial. The further issue with being so reliant on private actors in the collection and preservation of potential electronic evidence is ascertaining the reliability of the evidence. In traditional crimes, the investigation of a crime and handling of potential evidence is carried out by law enforcement agents who follow pre-determined protocols to ensure the integrity of evidence collected. One criticism levelled against private actors is that they are unprepared to ensure the same levels of integrity that is expected for a legal process. There is no legal framework so far that determines what level of 'forensic readiness' private actors should be expected to follow. As has been documented,[83] using mutual legal assistance to obtain information or electronic evidence from private actors is often very challenging for LEAs. Several issues have been identified: (1) mutual legal assistance requests are not specific and precise enough to enable companies to reply rapidly and efficiently; (2) services on mobile devices, based on apps; (3) data retention; and (4) difficulties with obtaining evidence on certain types of technologies, such as blockchains and virtual currencies.

[82] See for example the Google Transparency Report, available at https://www.google.com/transparencyreport/ and the Vodafone Law Enforcement Disclosure report, available at https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html?.

[83] See for example James and Gladyshev (2016), p. 23–32.

Apart from the EIO Directive and the Council of Europe Convention on Mutual Assistance in Criminal Matters, the Cybercrime Convention applies in cases where the crimes involved are cybercrimes. One of the weaknesses of the Convention is that it does not clearly provide for the real-time collection and/or interception of traffic and content data when the alleged content is outside the jurisdiction of the state investigating a particular crime. According to the Convention, competent authorities are empowered to collect or record traffic data transmitted by a computer system by technical means in real-time (Article 20 Convention). The competent authority may also compel a service provider to collect or record or to cooperate and assist the competent authorities in the collection or recording of traffic data. The collection or recording should be related to specified communications and within the territory of the state where the competent authority is located. If general principles of domestic law prevent the State Party to do so, it shall take other measures necessary to ensure the real-time collection or recording of traffic data. If a service provider is asked for assistance, the service provider is obliged to keep the execution of this power confidential. Cybercrime does not consider national borders, meaning that the data involved in cybercrime and the crime itself or the perpetrator are found extraterritorially to the investigating jurisdiction. In certain cases, the investigating jurisdiction may access the data regardless of the geographical location of the data without authorisation of the other jurisdiction based on Article 32 of the Cybercrime Convention. In all other cases, the investigating party is required to ask for mutual assistance, which is a time-consuming procedure.

Based on the international and European legal instruments and agreements, the extent to which states have tailored these general rules to the collection and sharing of electronic evidence varies greatly. In Italy, for example, in accordance with supranational agreements, Italian legislation explicitly covers cases in which national authorities are requested to collect or transfer evidence to another country (Article 723–726 ter CPC) and vice-versa (Article 727–729 CPC). These are general rules on evidence, but no specific rule exists on the cross-border exchange of electronic evidence. As for the Cybercrime Convention, Italy implemented this Convention with the Law 48/2008, which has not only introduced new types of crimes in the Criminal Code (CC) and has amended the Criminal Procedure Code (CPC) providing for new provisions on the use of new technologies (e.g. Article 254 bis CPC), but has also modified the existent provisions in the CPC and the CC to regulate cases in which electronic evidence is involved.[84] However, the provisions of the Criminal Procedure Code seem to contain less detailed or specific measures than the Cybercrime Convention. A similar situation can be found in Bulgaria where the general rules on international cooperation in criminal matters cover the collection of evidence. However, they do not provide for detailed rules. Apart from the obligations originating from the Cybercrime Convention, there are no specific national rules about requests and obligation to collect and/or

[84]For example Article 615 quinquies, 635 bis CC; Article 244 co. 2, 247 co. 1-bis, 254, 352 co.1-bis, 354 co. 2 of the Italian CPC.

transfer electronic evidence to authorities of another country. It can be said that Cybercrime Convention has been fully implemented into national law in Bulgaria.[85] As for similar constitutional traditions, the international treaties in Bulgaria, which have been ratified in accordance with the constitutional procedure, are part of the legislation of the state. The related norms have primacy over any conflicting provision of domestic legislation, i.e. the provisions of the Convention prevail in case of conflict with national provisions, including the rules on procedural law. Germany has also ratified and implemented the main international and European agreements, such as the Act on international cooperation in criminal matters[86]; Act on bilateral treaty between Germany and the USA about mutual assistance in criminal matters.[87] and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.[88] As for the Cybercrime Convention, it can be said that it has been implemented only partially in Germany, at least as far as the procedural law is concerned.

11.3.2 Challenges and Shortcomings

Based on the status quo of national and international legislation in the collection, preservation, use and exchange of electronic evidence, the challenges and shortcomings of the legal frameworks within the EU become apparent. These challenges and shortcomings include legal and data protection issues, problems with law enforcement particularly cross-border cases when evidence needs to be exchanged and technical issues in training and technical capabilities.

While criminal law is regulated at national level, it is inevitable to have some overarching international regulations and agreements. Not only considering globalisation and modern technologies and because crimes—both 'regular' crimes

[85]The relevant provisions include Article 125, 159, and 163 of the Bulgarian Criminal Procedure Code; Article 73, Chapter 15 on security and confidentiality of electronic communications networks and services, confidentiality of communications and data protection and Chapter 19 on ensuring conditions for interception of electronic communications related to national security and public order of the Electronic Communications Act; Special Intelligence Means Act and Article 90 of the Ministry of Interior Act.

[86]See: Gesetz über die internationale Rechtshilfe in Strafsachen (IRG).

[87]Available at: http://www.bgbl.de/banzxaver/bgbl/stArticlexav?start=//*[@attr_id=%27bgbl207034.pdf%27]#__bgbl__%2F%2F*[%40attr_id%3D%27bgbl207034.pdf%27]__1409231444625.

[88]See: Gesetz zu dem Übereinkommen vom 29 Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union. If there is no bilateral treaty that governs the legal assistance between the Federal Republic of Germany and the partner country, the IRG applies subsidiarily to countries outside the EU (§38 IRG and §39 IRG) and to Member States of the EU (§88 ff: Confiscation and Deprivation, §94 IRG: Request for sequestration, §97 IRG: Requests for passing on of evidence). Available at http://www.gesetze-im-internet.de/englisch_irg/index.html.

and cybercrimes may be committed across borders, but also considering the very nature of electronic evidence, particularly cybercrimes, and that it may be found anywhere in the world. The fact that criminal law is regulated at national level makes this problematic as all countries have different rules, procedures and approach. In certain countries traditional investigative powers might be general enough to apply to cases involving electronic evidence while in other countries traditional procedural laws might not cover such issues, making it necessary to have additional specific legislation. In both cases legislation requires a clear scope of application of powers and sufficient legal authority for actions.[89] Although Europe scores reasonably high on the sufficiency of national law for investigations, the main gaps in investigative powers include the lack of power to enter electronic networks to search for evidence and the lack of power to preserve computer data to support existing search powers.[90] There is thus a lack of harmonisation in substantive and procedural provisions, different approach to jurisdictional coverage of substantive and investigative provisions and there are different powers of investigation and enforcement. This makes it particularly difficult when the crime is committed in or has effects in several jurisdictions.

While a crime may be reported locally, the offence may have been initiated outside national boundaries or have some cross-border dimension, meaning that evidence may be found across borders, particularly cybercrime. Cybercrime is a global problem, meaning that law enforcement must adopt a coordinated and collaborative cross border approach to respond to this growing threat.[91] Enforcement can thus go from a local to a global level and back to local level (e.g. where the start of an investigation starts at a local level following a report by a victim in the state where the law enforcement agency is placed, then ask for evidence to be collected and retained by a foreign agency and then using that evidence in the prosecution of a crime in the Courts of the requesting state). This local-global-local process requires an effective legal framework that allows this process to happen. An effective enforcement scheme is required to prevent, detect and investigate crimes. However, the differences in national legislation and approach are problematic for law enforcement particularly concerning successful international cooperation. Although international cooperation has proven successful, there are few realities that need to be faced as coordination is costly and difficult to carry out for trivial matters such as time zone differences and nuances of local laws and customs in the jurisdictions involved.[92] Furthermore, technologies are developing rapidly and policing technologies need to be revolutionised with it, especially

[89] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 122, 123.

[90] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 124.

[91] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 9.

[92] See Gragido et al. (2013), p. 137.

considering the growing importance of electronic evidence. However, not all police forces may be equipped to handle such evidence. Finally, and probably most importantly, because of this local-global-local dimension of international crimes there are different levels of law enforcement involved and international cooperation and the exchange of evidence usually takes place via international actors such as Interpol or Europol. There is generally no direct contact between the local law enforcement authorities making the process slow and more difficult.

While there have been certain initiatives to bridge the gaps, including by the EU and Council of Europe, limitations remain. While certain of the international instruments attempt to provide for a basic level of harmonisation and standards for international cooperation there are still several limitations. Not all countries over the world are part of European initiatives, certain international instruments allow for reservations, diminishing their effect, difficulties with electronic evidence, jurisdiction, enforcement procedures, difficulties in enforcement, possible infringements of fundamental rights, etc. Existing legislative and enforcement frameworks and the concepts enshrined therein, as well as data protection concepts, precede the creation of the internet as we know today and do not satisfactorily deal with the realities of technological developments. Certain crimes do not consider national borders, the (electronic) evidence involved and the crime itself or the perpetrator may be found extraterritorially. This requires international cooperation, which may prove difficult in some cases because of differences in national enforcement legislation and approach. This is further difficult considering that electronic evidence is increasingly held by the private sector and that there is a general lack of legislation and uniform procedures to collect this evidence. Cybercrimes for example are rarely only EU-based as in many cases they involve third countries' companies (e.g. from the USA). Given that third countries do not seem to be very cooperative with European LEAs when asked to provide information or evidence on a crime and the European Convention on Mutual Assistance in Criminal Matters might not be invoked, a way out may be identified in making sure that LEAs are trained so that specific and precise (legal or technical) questions to third countries' companies can be asked and that companies may be able to reply more rapidly and efficiently. A better cooperation with ISPs and standard procedures or format to facilitate investigations in the collection of electronic evidence from the private sector is necessary. In many cases companies provide access to data but they deliver it as printouts of thousands of documents that require further investigation and efforts. It would therefore be useful to establish a common regulation at EU level on how companies are obligated to deliver their data in particular standard format. The formats would depend in the type of data (text, audio, video, etc.). Criminal investigations are too much in the hands of the willingness of a particular provider to provide the investigation with crucial information on traffic data, on subscription information or the personal data that may reveal an individual's doings on the internet. A further problem of obtaining electronic evidence from ISPs is represented by the growing world of services on mobile devices, based on apps. While before it was quite simple to identify the ISP to ask information nowadays, every app producer, in theory, can become a service provider but at the same time

not be viewed as a service provider in legal terms. It may be unclear, for each mobile service, what the internal structure of the database is or how the data is distributed and copied. The problem with this kind of entities not being recognised as service providers is in the non-applicability of the corresponding legal duties. ISPs have particular obligations, e.g. when it comes to providing data to LEA authorities as defined by (some) national data retention laws. All this electronic evidence needs to be preserved in terms of implementation of adequate archival procedures of (long-term) preservation of electronic records that might one day become evidence and proactive preservation of collected electronic evidence during the prosecution period. There is a general lack of standards in this regard and data retention periods vary across Europe, which is a main challenge that requires more harmonisation.

After the evidence is collected it will eventually need to be used in Court. One of the major challenges in this regard is lack of knowledge within the judiciary. Judicial actors need to be trained so that a minimal knowledge on electronic evidence and on its use in the judicial system is guaranteed, which would reduce the waste of time and resources in, for instance, translating investigation results from LEA to other judicial actors. It would be useful to clarify how the use of offensive technologies by LEAs to acquire data is compatible with the rules of law, notably, to clarify what lawful interceptions are (if we consider the use of sophisticated technologies). To investigate efficiently an alleged criminal, it may be necessary for LEAs to act in an offensive manner by performing intrusion on criminals' systems or internet networks used by criminals or find other ways to intercept message and data exchanged to and from criminals' system. Without a clear definition at the EU level of what is allowed for LEA, sometimes an investigation cannot take place. In the virtual world, investigations cannot follow the same model as in real physical world, for instance, because there is the possibility of making identical copies. While in the physical world when an object is seized it can be returned to the owner after the judicial process in the same state, virtual things (e.g. virtual currencies) could change over time. Currently, there is no legislation on acquiring virtual currencies that may evolve over time. For example, a bitcoin may completely change in value during the investigation and the question is who is responsible for the loss or benefits.

11.3.3 Criteria for Uniform Regulation

Solving the current shortcomings is not merely a matter of introducing new agreements or a better harmonisation of rules on electronic evidence. The situation is arguably more complex, needing new theoretical frameworks and the collaboration of a large variety of actors. When identifying the challenges and shortcoming concerning the collection, preservation, use and exchange of electronic evidence the question arises whether the EU should move towards a uniform set of rules that facilitate the exchange of electronic evidence across borders; "What should be harmonised, if at all?". To answer this question reflections on the current rules on

collection, preservation and use of electronic evidence around Europe; and existing rules on transfer and exchange are necessary.

Before embarking on answering this question it is important to remember that all Member States have at least one important basis in common: protection of fundamental rights. The collection, preservation, use and exchange of electronic evidence can only be sound and effective if it is based on fundamental rights and freedoms and individuals' rights cannot be secured without safe networks and systems. Law enforcement, prosecution and the judiciary should execute investigative powers and procedures with regard for human rights and liberties. Protecting fundamental rights, freedom of expression, personal data and privacy are of utmost importance. Therefore, security, investigative and procedural measures need to be proportionate and guided by core values such as human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. Fundamental rights, democracy and the rule of law need to be protected in cyberspace while protecting against incidents, malicious activities and misuse. These rights and freedoms also include the right to a fair trial, particularly when preparing a defence case where electronic evidence forms part of the evidence. All Member States provide for the codification of fundamental rights. Any common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should be based on the protection of fundamental rights and freedoms, including proper restrictions and safeguards. The basis for this already exists in the Member States of the EU through the ratification of the ECHR and through constitutional provisions and traditions in the different Member States.

11.3.3.1 Should the Prevailing Rules on Collection, Preservation and Use of Electronic Evidence in Europe be Harmonised?

Legal Basis and Uniform Definitions, Concepts and Standards

The collection, preservation, use and exchange of electronic evidence should be based on clear and precise legislative provisions. This is currently embedded within the national laws of the Member States. All Member States provide a legal basis for investigative measures, be it traditional or specialised laws, and all Member States allow applying general rules of (traditional) evidence to electronic evidence. However, there is no uniform regulation, no standardisation and use of definitions.

So far there is no evidence that a lack of a common definition of what is electronic evidence has kept Member States from working together on the collection, preservation and use of electronic evidence. Neither is there evidence that the lack of a definition of what constitutes 'evidence' in the European Convention on Mutual Assistance in Criminal Matters, has been an impediment for the mutual assistance between European countries. While, in theory, having a uniform definition of electronic evidence may be of assistance to facilitate the process of exchange of electronic evidence, this is dispensable for the collaboration between Member States. The definition developed and used in the EVIDENCE project mentioned at the beginning of this chapter may be a useful point of departure: *electronic evidence*

is defined as "any information (comprising the output of analogue devices or data in digital format) of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device".[93]

Common and Specific Rules, Definitions, Standards and Procedures of Collection

While some Member States may have certain specialised technical provisions in the collection of electronic evidence, all Member States (also) apply the rules, concepts and procedures for traditional evidence apply to electronic evidence. These rules, concepts and procedures in many cases may however be outdated and not equipped for electronic evidence, which leads to enforcement issues and possibly to admissibility issues, particularly cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should be based on clear and specific rules for the collection of electronic evidence, common definitions and standards and approximation of legal procedures.

It can also be argued that what is needed is not uniform legal rules for collection (as a legal basis for collection exists already in all Member States) but rather operational guidelines or rules on the actual handling of electronic evidence. While all Member States have within their country certain specific agencies or units, particularly forensic institutes, specialised in the collection, examination and preservation of evidence, there are limited guidelines or procedures for the use of digital technologies in criminal proceedings. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should include a plan for the development of common guidelines and procedures.

Collection of evidence by private sector actors and the passage of electronic evidence from the private sector and LEAs also needs to be addressed. It is increasingly evident that a large part of electronic evidence originates from private sector actors, e.g. ISPs providing traffic data of internet transactions, telecommunications providers providing information on mobile communications, etc. There is currently no national framework that clearly regulates this relationship and the origin, collection and use of electronic evidence from the private sector. This is a gap that a common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence can address.

Guidelines for Preservation and Use

Apart from the provisions in the Cybercrime Convention (and as implemented by the States Party to the Cybercrime Convention) on expedited preservation of data stored on a computer and of traffic data, there is a general lack of specialised regulation across Europe concerning preservation methods and use, including standards or

[93]Definition used in the EVIDENCE Project—Deliverable 2.1—EVIDENCE Semantic Structure, p. 18.

guidelines on who is authorised to process the electronic evidence in what stage of the criminal proceeding and access restrictions, specifications on how the evidence must be preserved and how to handle evidence obtained from private companies. In line with the suggested position for rules on the collection of electronic evidence a common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence need to include legislative and other measures, including guidelines on the preservation of electronic evidence, and including rules on access restrictions, authorisation, method and duration of preservation, data protection, and other rules. Furthermore, where any of the tasks of preservation and examination of electronic evidence is to be carried out by private sector actors, additional safeguards are to be put into place to ensure the proper preservation and retention of electronic evidence.

Specific Investigative Measures
Not all Member States cover certain interception and search and seizure methods (that lead to electronic evidence) within their national legal frameworks. Where rules exist these follow from the provisions of the Cybercrime Convention and apply mostly to the investigation of cybercrimes. Most of the Member States extend the application of traditional investigative methods to electronic evidence. While in some cases this might work, generally these methods do not sufficiently cover the specific nature of electronic evidence collection. A more specific legal basis is necessary to obtain electronic evidence, particularly to avoid admissibility issues in cross-border cases. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence should thus include specific, clear and precise investigative measures in the collection of electronic evidence.

Admissibility Based on Mutual Trust
Admissibility of electronic evidence is generally not an issue and electronic evidence is generally admissible if it has been legally obtained and is assessed on a case by case basis by the Court. However, given that the requirement of 'legally obtained' is not a uniform requirement (e.g. in Sweden the principle of free evaluation of evidence, meaning that evidence is not refused on the ground of how it was collected, prevails), the non-uniform approach may be a barrier for the use of electronic evidence obtained from another jurisdiction. It is thus important to set common standards in this regard. While the probative value of the evidence is not diminished because of the electronic nature of the evidence and collection, preservation, use and exchange of electronic evidence in criminal proceeding is generally not restricted or prohibited by law, the very nature of electronic evidence makes it volatile and easy to manipulate. Common standards for maintaining the integrity of the electronic evidence are therefore necessary while at the same time electronic evidence obtained in one Member State should not have any difficulties with admissibility in another Member State.

There may be two approaches here: either the drafting of common rules on that admissibility of evidence (in the cross-border context) or an agreement that the law of the requested state (that is the law of the state providing the evidence to a

requesting state) prevails in the context of cross-border situations. It is then still up to the Court of the requesting state to decide whether to admit the evidence to the proceedings or not. This concept of following the law of the requesting state is a concept familiar to both the Cybercrime Convention and to the European Convention on Mutual Assistance in criminal matters.

Regulation of Cloud Computing
There is hardly any regulation across Europe concerning cloud computing and electronic evidence that is stored or located in the cloud. Considering the growing importance of cloud services, a common European framework should include specific provisions in the collection of electronic evidence out of a cloud service. This rule should go further than the search and seizure rules (for electronic evidence) that exist in the Cybercrime Convention, as the current rules are bound to the territorial jurisdiction of the state where the investigation is taking place. Rules on the obtaining of evidence from the cloud need to go beyond the current limitations of territorial jurisdiction. One possible way is to agree on a 'universal jurisdiction' approach in the investigation of serious crimes.

11.3.3.2 Should the Prevailing Rules on the Transfer and Exchange of Electronic Evidence in Europe be Harmonised?

Transfer of Electronic Evidence
It is remarkable how little regulation there is concerning the transfer and exchange of electronic evidence within domestic boundaries and internationally. One would expect that states would have clear rules on transfer considering the volatile nature of electronic evidence and the large potential of tampering with the evidence during the electronic evidence's lifecycle that could lead to the inadmissibility of the evidence and/or could impact the fundamental rights of suspects and/or victims. This is clearly not the case. Most Member States rely on, where available, rules for the transfer of evidence between actors in the evidence chain of custody. Most of the rules that exist, where they exist have been prepared by some of the prominent actors themselves, e.g. most national forensic institutes have rules on the receipt and transfer of electronic evidence to be examined by them.

Provisions to Regulate the Role of Private Sector Actors
Furthermore, the lack of rules on exchange of electronic evidence is even more critical in the transfer of electronic evidence to or from private actors. Increasingly, as already noted, electronic evidence originates from private sector actors, and increasingly digital forensics expertise is more common in the private sector than in the public sector. This creates dependence in many states of LEAs on private actors for the collection, examination and preservation of electronic evidence. There are at least three main reasons that militate in favour of harmonised rules on the transfer of electronic evidence within a domestic space and further internationally:

1. An increased reliance on electronic evidence as primary or main source of evidence for crimes previously having no link with an electronic reality. There is an exponential increase of the collection, use and preservation of electronic evidence in trials or criminal law proceedings where previously electronic evidence may not have been thought of (e.g. there is hardly any murder trial where for example evidence from a mobile phone does not play some part in the collection of evidence and building up of the case by the prosecution). This increased reliance requires a recalibration of resources within a LEA to meet with the demand and a better legal certainty on the legal processes for collection, transfer, exchange, use, examination and preservation.
2. Increase in use of electronic evidence collected by the private sector. As already pointed out, most of electronic evidence originates within a private sector context. It is important for LEAs to have clear rules of what categories of data can be obtained from the private and what procedures need to be followed. Requests by LEAs to the private actors generally take a long time to be answered or acted upon, if at all. A common framework may include, inter alia, a list of 'open' information across Europe and ways LEAs can access this information, rules on uniformity to access telecommunications information and/or highly demanded categories of information, rules on how LEAs in one Member State can directly ask a telecom company in another Member State for specific categories of information and rules on how the transactions between the private companies and LEAs are carried out, including audit trails.
3. Increase in use of private sector expertise for the analysis and examination of electronic evidence. With the increase in use of electronic evidence, national forensic institutes (if they exist at all within Member States) cannot meet all the demands or requests for the analysis of electronic evidence. This creates a demand for private sector experts to carry out the analysis and to give expert testimony before Courts. So far there are no rules in Member States on the transfer of the electronic evidence to the private sector experts nor on the responsibilities of experts. Traditional domestic rules on expert witness have often been extended to cover expertise on electronic evidence. A common framework needs to include rules on the engagement of private sector experts and on the way the electronic evidence is transferred to and from private sector experts.

Transfer of Actionable Intelligence from Intelligence Agencies and LEAs and Vice-Versa

So far, the transfer of information or actionable intelligence between SIS and LEAs and vice-versa, where this happens, is often not regulated. Few states, amongst which Germany, have clear rules on the transfer of information between the two. Especially following the Snowden revelations there seems to be an on-going debate questioning the previously 'water-tight' distinction in legal treatment (and application of laws) to law enforcement and security services/ intelligence agencies. It becomes increasingly obvious that the distinction is less water-tight then has been portrayed so far (and which is furiously fought over especially by

security services/intelligence agencies). As Cannataci argues in "Defying the logic, forgetting the facts: the new European proposal for data protection in the police sector", "In many states SIS do not have executive powers, although there do exist a few exceptions especially in the case of anti-terrorist activities. However, in most cases the prime function of the SIS is to produce "actionable intelligence", which is then passed on to the LEAs to act about whether it is to further monitor, follow, detain, arrest or prosecute a person or group of persons." Given this context, it may be opportune to include in a common European framework for electronic evidence rules on the transfer and exchange of information/actionable intelligence and whether this information can be admitted as evidence in a criminal trial.

Effective Cross-Border Regulation
The whole process of exchange of evidence between states in Europe is based on mutual legal assistance bilateral agreements, the European Convention on Mutual Legal Assistance in Criminal Law Matters, the EU 2000 Convention, which was recently replaced by the EIO Directive and for evidence related to cybercrimes, the provisions of the Cybercrime Convention. All these legal frameworks have been used for the exchange of electronic evidence. However, it is increasingly evident that (apart from the provision of the Cybercrime Convention) the procedures offered in these frameworks are too slow for the volatile and fast-moving nature of electronic evidence. The provisions and procedures in the Cybercrime Convention are better suited for electronic evidence but States have often not extended their application beyond the scope of the Cybercrime Convention when ratifying the Convention. A common European framework for the systematic and uniform application of new technologies in the collection, use and exchange of electronic evidence can build on the existing provisions and procedures in the Cybercrime Convention. Furthermore, a common European framework could take up and build on the current efforts of the Council of Europe to create an electronic version of the mutual legal assistance request form.

Joint Investigation Teams
Under the auspices of Europol and Eurojust, several JITs have been set up during investigations. These joint investigations allow for an efficient way of collecting and sharing of electronic evidence pertinent in an investigation. A common European framework may need to increase the legal certainty needed for such joint investigations to be carried out in a smoother and more efficient manner.

11.4 Conclusion

Over time, the European legal scenario regulating the life cycle of electronic evidence has evolved in a complex patchwork of rules. As to the setting up of rules on collection and preservation of electronic evidence, the Cybercrime Convention has been the most influential and progressive framework for electronic evidence in Europe. Many national frameworks are a combination of national criminal law

provisions developed in the off-line context and provisions that were introduced through the ratification of the Cybercrime Convention. While this combination brings some degree of uniformity, the national criminal law approaches remain the primary source for the rules on admissibility and probative value of electronic evidence.

The most evident deficiency in the current patchwork is the inability of current national and international legal frameworks to meet the needs that come from the 'cross-border' nature of electronic evidence. As this chapter has discussed, the current prevalent notions of jurisdiction, particularly as the notion governing investigative powers is rather limiting and problematic in today's world where electronic information is processed, shared and stored across several territorial jurisdictions and spaces. Here new theoretical frameworks, such as the notion of 'investigative jurisdiction', are being proposed in literature but are still not in practice.

One scenario where this notion of 'investigative jurisdiction' may be less useful is when requiring information directly from a private actor: which rules would the private actor be expected to follow (of location or of the investigating party) is not immediately clear and would still be dependent on some form of legal agreement.

One other aspect that needs to be rethought in the context of (cross-border) electronic evidence is the notion of admissibility of evidence. Admissibility of electronic evidence is generally not an issue and electronic evidence is generally admissible if it has been legally obtained and is assessed on a case by case basis by the Court. However, given that the requirement of 'legally obtained' is not a uniform requirement the non-uniform approach may be a barrier for the use of electronic evidence obtained from another jurisdiction.

What needs further reflection is the role of private actors in the electronic evidence life cycle. While literature is replete with recommendations that a better cooperation with the service providers is desirable, there are no clear recommendations on how this cooperation should be developed. Improving mutual legal assistance requests and the way the requests reach the private actors is important and increasingly urgent. The legal framework for legal assistance requests while unsatisfactory for today's requirements, shows that establishing a clear legal process is very important in cross-border relations between states in criminal matters. Learning from this principle and corroborated by the findings of the EVIDENCE project, one can clearly establish that there is a need for electronic information/evidence exchange protocols and standards. These protocols need to have a legal basis, ideally internationally agreed and accompanied by a technical protocol for the fast transfer of the requested information exchange. Given further that these protocols and standards need to work not only between states but also between law enforcement agencies and several private actors, different stakeholders (including digital forensic experts) are involved in the process of setting up these protocols and standards.

In conclusion, while the current frameworks provide an important basis upon which law enforcement and prosecutors work, solving the current shortcomings is not merely a matter of introducing new agreements but is more complex, needing new theoretical frameworks and the collaboration of a large variety of actors.

References

Brenner SW, Koops BJ (2004) Approaches to cybercrime jurisdiction. J High Technol Law 4(1):46
Chalmers D, Davies G, Monti G (2010) European Union law. Cambridge University Press, Cambridge, p 582
Gragido W, Molina D, Pirc J, Selby N (2013) Blackhatonomics - an inside look at the economics of cybercrime. Syngress (Elsevier), Waltham
James JI, Gladyshev P (2016) A survey of mutual legal assistance involving digital evidence. Digit Investig 18:23–32
Jerker D, Svantesson D, van Zwieten L (2016) Law enforcement access to evidence via direct contact with cloud providers - identifying the contours of a solution. Comput Law Secur Rev 32:671–682
Koops BJ, Goodwin M (2014) Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law, December 2014. https://www.wodc.nl/onderzoeksdatabase/2326-de-gevolgen-van-cloudcomputing-voor-de-opsporing-en-vervolging.aspx?cp=44&cs=6796
Mason S (2012) Electronic evidence, 3rd edn. LexisNexis Butterworths, London
Shaw MN (2008) International law. Cambridge University Press, Cambridge
Svantesson D (2016) Law enforcement cross-border access to data, Preliminary Report, November 2016