Универзитет „Гоце Делчев“-Штип, Правен факултет
Штип, Република Македонија

ЧЕТВРТА МЕЃУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА

ОПШТЕСТВЕНИТЕ ПРОМЕНИ ВО ГЛОБАЛНИОТ СВЕТ

ЗБОРНИК НА ТРУДОВИ

Штип, 2017

Печати / Print 2-ри Август-Штип / 2- ri Avgust- Shtip
Уредник: Елена Максимова

CIP - Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

3(082)

МЕЃУНАРОДНА научна конференција Општествените промени во глобалниот свет (4 ; Штип)
Општествените промени во глобалниот свет : зборник на трудови / Четврта меѓународна научна конференција = Social change in the global world : proceedings / 4 th international scientific conference = Социальные изменения в глобальном мире : сборник материалов / Четвертый международная научная конференция. - Штип : Универзитет Гоце Делчев = Shtip = Goce Delcev University = Штип = Университет Гоце Делчева, 2017. - [1210] стр. : табели ; 25 см

Трудови на мак., англ. и рус. јазик. - Фусноти кон текстот. - Библиографија кон трудовите

ISBN 978-608-244-423-9

а) Општествени науки - Зборници
COBISS.MK-ID 103854858

Goce Delcev University in Shtip, Faculty of Law
Shtip, Republic of Macedonia

FOURTH INTERNATIONAL SCIENTIFIC CONFERENCE

SOCIAL CHANGE IN THE GLOBAL WORLD

PROCEEDINGS

Shtip, 2017

Университет им. Гоце Делчева, Юридический факультет
Штип, Республика Македония

ЧЕТВЕРТЫЙ МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ

СОЦИАЛЬНЫЕ ИЗМЕНЕНИЯ В ГЛОБАЛЬНОМ МИРЕ

СБОРНИК МАТЕРИАЛОВ

Штип, 2017

Организациски комитет / Organizational Committee/ Организационный комитет конференции

Jovan Ananiev PhD, Faculty of Law, University "Goce Delcev"- Shtip, Macedonia, jovan.ananiev@ugd.edu.mk
Kristina Misheva PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, kristina.miseva@ugd.edu.mk
Marija Ampovska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, marija.radevska@ugd.edu.mk
Elena Maksimova, LL.M, Faculty of Law, Goce Delcev University in Shtip, Macedonia, elena.ivanova@ugd.edu.mk

Програмски комитет / Program Committee / Программный комитет конференции

Adoyi Onoja PhD, Nassarawa State University, Keffi, Nigeria, onojaa@yahoo.com
Afet Mamuti PhD, Faculty of Law, State University of Tetovo, Macedonia, afet.mamuti@unite.edu.mk
Agim Nuhiu PhD, Faculty of Law, State University of Tetovo, Macedonia, agim.nuhiu@unite.edu.mk
Agor Sarkisyan PhD, University of Svishtov, Bulgaria, agop@uni-svishtov.bg
Alenka Verbole PhD, currently- OSCE Mission in Tirana, University of Ljubljana, Slovenia, alenka.verbole@osce.org
Altin Shegani PhD, Faculty of Law, University of Tirana, Albania, altin_shegani@yahoo.com
Ana Nikodinovska Krstevska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, ana.nikodinovska@ugd.edu.mk
Anastasia Bermúdez Torres PhD, Faculty of Law, Political Science and Criminology, University of Liege, Belgium, abermudez@ulg.ac.be
Andon Majhoshev PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, andon.majhosev@ugd.edu.mk
Bekim Beliqi PhD, University of Prishtina, Department of Political Science, Kosovo, bekim.baliqi@gmail.com
Belul Beqaj PhD, University of Business and Technology, Department of Political Science, Prishtina, Kosovo, belul.beqaj@gmail.com
Borka Tushevska PhD, Faculty of Law, Goce Delcev University in Shtip, Macedonia, borka.tusevska@ugd.edu.mk
Elena Ivanovna Nosreva PhD, Faculty of Law, Voronezh State University, Russia, elena@nosyreva.vrn.ru
Gabriela Belova PhD, Faculty of Law, University "Neofit Rilski", Blagoevgrad, Bulgaria, gbelova@hotmail.com
Gemma Andreone PhD, Institute for International Legal Studies of the Italian National Research Council (ISGI - CNR), Italy, gemma.andreone@gmail.com

Содржина

EUROPEAN UNION'S CROSS-BORDER COOPERATION IN EXCHANGING AND PROCESSING DIGITAL EVIDENCE

Ivica Josifovic

Associate Professor, PhD

Faculty of Law, Goce Delcev University - Shtip

e-mail: ivica.josifovik@ugd.edu.mk

Abstract

We live in an online world. Everything we do is connected with the use internet. The Information and Communication Technology has developed so much and contributed towards economic and social benefit. But, on the other side, terrorists and cybercriminals are using cyberspace to criminal actions. Such problem is not local and for single country; it is global and therefore needs a global approach to tackle such criminal actions.

Therefore, law enforcement authorities should be able and supported to effectively conduct investigations against terrorist acts and terrorist groups using the information and communication technology. But, there is an issue of territorial jurisdiction, because of the internet and its no-border nature. Questions arise regarding the data that could be used as evidence in courts and the judicial cooperation, as well as the privacy protection of citizens.

The Council of Ministers of the EU in June 2016, stressed out the significance of improving the effectiveness of criminal justice in cyberspace. In its conclusions, the Council provides a starting point and the paper seeks to answer several questions: What are the main challenges that EU and member states face today when they collect e-evidence? How are they tackling these issues (explained through case studies)? Can an EU common framework provide solutions to solve these problems?

Keywords: *European Union, cyber-crime, electronic evidence, exchange, process*

1. Introduction

The collection of e-evidence – defined as data that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system that is relevant to the judicial process – is becoming more and more relevant in criminal justice to successfully prosecute not only cybercrime but all criminal offences.

The EU Council in June 2016 emphasized the need of e-evidence collection and their use in criminal procedures concluding that such an improvement should occur through enhanced cooperation with service providers, reorganization of mutual legal assistance proceedings, and review of the rules to enforce jurisdiction in cyberspace.[1] The mutual recognition principle became a key element in Europe's cooperation in criminal matters and the introduction of the European Investigation Order (EIO) is a significant step forward.[2] Basic documents for securing e-evidence throughout member-states are the Council of Europe's Convention on Mutual Assistance in criminal matters,[3] The Schengen Convention,[4] European Convention on mutual assistance in criminal matters and its protocols.[5]

The paper considers several issues. First, it explains the legislative framework of e-evidence at EU level. Second, it elaborates the digital relations EU develops with its partners, especially relations with the USA regarding e-evidence. Finally, the paper explains three case studies from national authorities of France, Germany and Italy regarding their legislative framework on e-evidence. The three cases studies look into member-state's legislations, law enforcement agencies investigation techniques and tools, relations with service providers and cross border data requests with other EU member states and the USA.

First, in the context of the fight against crime, law enforcement authorities should be fully equipped to effectively conduct investigations to prevent, detect and prosecute using information and communication technologies. In April 2015, the European Agenda on Security set three main security priorities: terrorism, organized

[1] Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9 June 2016.

[2] Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, May 1, 2014.

[3] Council of Europe, The European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959.

[4] Council of the EU, Council Decision Concerning the Definition of the Schengen Acquis, 20 May 1999, OJ L 176, July 10, 1999.

[5] Council of the EU, Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member states of the European Union, OJ C 197, July 12, 2000.

crime and cybercrime.[6] To investigate crime, competent judicial authorities should be able to enforce jurisdiction in cyberspace and obtain the evidence and information they require. Second, judicial cooperation should also be consolidated to allow national authorities to obtain data when it is found or moves across jurisdictions and stronger cooperation with service providers by concluding agreements or informal arrangements to exchange e-evidence in the context of crime investigations. However, the current international framework is not proving to be working effectively. Mutual legal assistance should be the most common solution for law enforcement authorities to gather cross border e-evidence, but it is turning out to be increasingly problematic. Procedures could take months due to bureaucracy, dual criminality and the absence of arrangements for expeditious actions. Therefore, carefully designed international frameworks might therefore be the best path to follow, instead of adopting domestic measures. Third, privacy should continue to be protected and citizens should not fear that their online data are accessed by authorities regardless of proper legal safeguards. An international framework might be upheld only if all the players involved respect and play according to the same rules. In this context, activities brought by Snowden affair have influenced ongoing discussions on the importance of ensuring privacy in cyberspace. Access to data should occur only in the context of crime investigations and under the safeguards and legal requirements of criminal procedure laws.

2. European Judicial cooperation and e-evidence in the EU

The existing legal framework in European judicial cooperation moves towards the mutual recognition principle in criminal matters, according which every judicial decision shall automatically be accepted in all other member-states and shall have the same or at least similar effect.[7] The principle aims at replacing the traditional forms of international cooperation, which are considered to be slow, complicated and insecure. EU was concrete in applying the principle by accepting the European Arrest Warrant in 2002, oriented towards replacement of the multilateral extradition system with enhanced and simplified procedure.[8]

The judicial cooperation in the EU developed in 1985 through the Schengen Area. With the removal of checks on their internal borders, EU became aware of the

[6] European Commission, The European Agenda on Security, COM(2015) 185 final, Strasbourg, April 28, 2015.

[7] European Commission, Mutual Recognition of Final Decisions in Criminal Matters (COM/2000/495), 26 July 2000.

[8] Council of the EU, Council Framework Decision 2002/584/JHA on the European Arrest Warrant, Brussels, 13 June 2002, OJ L 190, July 18, 2002.

need of effective pursue of criminals acting through member-states and anticipated series of court procedures for facilitation and enhancement of investigation in criminal matters. The Schengen acquis established the Schengen Information System for improvement of the efficiency in the fight against serious and organized crime. Interestingly, the Schengen Convention emphasized the importance of pre-trial measures, stressing out that the "data on objects sought for the purposes of seizure or use as evidence in criminal proceedings shall be entered in the Schengen Information System."[9]

The European Convention for Mutual Assistance in Criminal Matters from May 2000 represents a first major step in judicial cooperation, including the collection of evidence. The Convention regulates relevant points, reaching from wide use of new technologies, including the interception of communications which may be intercepted or directly transmitted to the requesting state or recorded for further transmission. Additionally, it emphasizes the "spontaneous exchange of information", according which, without a mutual assistance request, national authorities are authorized to exchange information regarding criminal offences.

The Council's Framework Decision from 2003 on the execution of orders freezing property or evidence[10] and the Council's Framework Decision from 2008 on European Evidence Warrant (EEW)[11] are included in the EU's legal frame for guiding the sensitive area of cross-border collection and use of evidence in criminal proceedings. However, e-evidence does not fall neither under the EEW, neither under the Framework Decision on the execution of orders freezing property or evidence.

The Council of Europe is the first to address the potential challenge regarding e-evidence for police and judicial cooperation by adopting the Budapest Convention in 2001.[12] The Convention attempts to address the criminal procedure issues regarding information technologies, thereby securing legal frame for providing e-evidence collection. In urgent cases, "expedited means of communication, including fax or e-mail" are understood as accelerators of the evidence collection process, according Article 25, paragraph 3. More importantly, specific provisions, especially Article 29, authorize "expedited preservation of stored computer data" before formal

[9] Council of the EU, The Schengen Acquis Integrated in the European Union, OJ L 239/1, September 22, 2000.

[10] Council of the EU, Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence, 22 July 2003, OJ L 196/45, August 2, 2003.

[11] Council of the EU, Council Framework Decision 2008/978/JHA on the European Evidence Warrant, 18 December 2008, OJ L 350/72, December 30, 2008.

[12] Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001.

request on mutual assistance is being made. Further, the Convention in Article 31, paragraph 1, deals with cases of mutual assistance regarding the access to stored computer data "located within the territory of the requested Party", thus enabling, according Article 32 "trans-border access to stored computer data with consent or where publicly available". In order to speed up the judicial cooperation in criminal matters, the Convention in Article 35, paragraph 1, provides a 24/7 network, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings. Further, the "production order", from Article 18, also, presents important measure as it covers the applicability of domestic orders outside the territory, such as "to submit specified computer data … stored in a computer system". However, the Budapest Convention, ratified by 49 states, including 25 EU member-states, remains limited in its extent as it applies only on cybercrime.

In order to secure collection and exchange of e-evidence, it is necessary for the communications and internet providers to make such data available to authorities. After 2004 Madrid attacks, EU sought the importance of controlling this area.[13] Seeking harmonization of data retention provision, in March 2006 the EU adopted the Directive on data retention.[14] As stipulated in Article 3, it applies on "providers of publicly available electronic communications services or of a public communications network" and, as stipulated in Article 5, only for subscriber and traffic data. Article 6 provides that data retention is left on member-states for a period not shorter than six months and no longer than two years. Finally, as the Preamble states, data should be used exclusively for the purposes of "prevention, investigation, detection and prosecution of criminal offences". Despite the importance of data retention, in April 2014, the Court of Justice annulled the Directive regarding the right to private life and right on protection of personal data.[15] According the Court, the non-discriminate data retention of legal and private persons may constitute a permanent surveillance, directly in opposition of the right on privacy.

While the criminal justice strengthens, EU acknowledged the importance of human rights and rule of law in cyberspace. Considering the need of adaptation of EU legislation for data protection in cyberspace, the EU undertook comprehensive package of reforms in order to secure protection of personal data. Three significant reforms on rules for protection of data are highlighted.

[13] Council of the EU, Declaration on Combating Terrorism, Brussels, 25 March 2004.

[14] Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105/54, April 13, 2006.

[15] Court of Justice of the EU, Judgement of the Court in Joined Cases C-293/12 and C-594/12.

The General Data Protection Regulation, which entered in force in May 2016 and shall start to apply from May 2018, secures a high level of personal data protection and regulates the transfer of personal data for commercial purposes.[16] This regulation is complemented by Criminal Law Enforcement Data Protection Directive, which specifically applies on processing personal data in the police and judicial sector.[17] This, so-called "Police Directive" shall secure personal data protection transferred for the purposes of e-evidence in criminal investigations. It establishes specific rules for data exchange in the area of prevention, investigation, detection and prosecution of crime offences, as well as the execution of crime sentences. When relevant authorities face with different tasks then these mentioned, data transfer falls under the frame of the Regulation. The Directive does not consider the police and judicial cooperation with third states, as it applies only on transferred data available among member-states. In this case, member-states remain capable to conclude bilateral agreements for data transfer in criminal proceedings. For other activities, such as national security, data transfer does not follow the General Data Protection Regulation or the Police Directive. In these cases, member-states apply domestic rules.

With the General Data Protection Regulation and the Police Directive in place, EU turns its attention on reformation of the Directive on Privacy and Electronic Communications (e-Privacy Directive).[18] This Directive establishes a strong prohibition for interception and record of electronic communications and retention of combined metadata for those communications. Also, Article 15 of the e-Privacy Directive establishes the limitations in EU member-states discretion to derogate from those commitments for law enforcement purposes. The e-Privacy Directive, aligned with the General Data Protection Regulation, shall be a central part of the EU thinking for acceptable mixing with the online privacy in the name of providing the law and public safety.

Existing EU instruments show fragmented legal framework in the area of judicial cooperation in criminal matters. Besides this background, the EIO, as a new

[16] Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and repealing Directive 95/46/EC, OJ L 119/1, May 4, 2016.

[17] Directive 2016/680 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/1, May 4, 2016.

[18] Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201/37, July 31, 2002.

instrument, is expected to be transferred in member-state's legal frame during 2017 in order to facilitate the judicial cooperation in criminal matters. Finally, the purpose of the EIO is to replace most of the existing instruments in this area, thus moving from mutual legal assistance to the mutual recognition principle. However, it needs to be stressed out that the territorial range of the Directive remains limited; not all member-states agreed upon the implementation.

Two major parts of the EIO Directive could be identified. The first section, Chapters from I to III, is facing general rules for support of the mutual recognition principle in the area of collection and exchange of e-evidence. The second section, Chapters from IV to VI, contains specific provisions for certain investigation measures, such as temporary transfer of evidence, videoconference hearing information on banking and other financial operations, undercover investigations and interceptions. According Article 1, paragraph 1 of the EIO, a state may issue such order regarding one or several specific investigation measures, which need to be executed in another state including, if possible, exchange of evidence. EIO in Chapter V includes collection or transfer of e-evidence, exclusively understood as electronic data received by interception of communications. As the EIO does not consider the collection or exchange of e-evidence which are not acquired through interception, call on data retention has not been made. Also, mandatory periods for recognition or execution are included; the decision for recognition or execution of the EIO, according Article 12, paragraph 3, must be taken no later than "30 days after the receipt of the EIO", while investigations, according paragraph 4, need to be undertaken by the executing state "not later than 90 days". Finally, grounds for refusal are clearly stipulated in Article 11 where, in addition to traditional restrictions concerns have been made on "national security interests".

3. E-evidence relations with the USA

The fight against cross-border crime should not be limited only on European borders and EU should cooperate with its partners, especially the USA. Regarding evidence collection, the EU-US framework agreement from February 2010 for facilitation of collection and information exchange, entered in force.[19] Among the most important innovations could be mention the "identification of bank information"

[19] Agreement on Mutual Legal Assistance between the European Union and the United States of America, Washington, 25 June 2003; Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America OJ L 291, November 7, 2009.

(Article 4), establishment of "joint investigation teams" (Article 5) and "expedited transmission of requests" (Article 7). One of the major obstacles for EU-US cooperation is the different understanding of criminal offences, as well as the length of different procedures. However, for e-evidence purposes and apart from the fact that most of the internet providers are located in USA, the transatlantic cooperation on collection of e-evidence remains problematic.

For this reason, the Council emphasized the need of accelerating the discussions for possible ways of secure and collection of e-evidence through the use of the already existing EU-US Agreement on mutual legal assistance. Further, after the Snowden affair, the concerns arise regarding the handling of European data by US authorities in the context of intelligence and law enforcement activities. Therefore, a US-EU Privacy Shield is adopted in June 2016 for protection of data use across the Atlantic.[20] The Agreement anticipates protection measures and supervision mechanism for limitations to data access by US authorities and confirms the absence of "indiscriminating or mass surveillance." Still, the Agreement is limited to personal data exchange for commercial purposes.

The EU-US Privacy Shield is supplemented by the EU-US Umbrella Agreement, which regulates the issue of transatlantic e-evidence exchange, thus establishing comprehensive framework for data protection in cyberspace.[21] The agreement, signed in June 2016, regulates the exchange of evidence for purposes of prevention, investigation, detection and prosecution of criminal offences, including terrorism, thus strengthening the data protection rights. Once operational, the Umbrella Agreement, according Article 3, shall protect all personal data exchanged between police authorities of EU member-states and US federal authorities. Further, according Article 19, it guarantees equal treatment for EU citizens, who will be able to enjoy the rights stipulated in the agreement. Therefore, as long as the cooperation in criminal matters strengthens, the protection and guarantees are also secured. For example, provisions for limitations of the data use and retention are included.

The adoption of general conditions regulating the data transfer represents a significant step forward regarding the protection of human rights; but the problem in collecting e-evidence should be more directly addressed. As mentioned, EU still has not covered this issue with common legislation and relies on mutual legal assistance procedures, as they are inappropriate and inefficient in the fight against serious crime. Based on territorial principle, in case of collecting e-evidence, mutual legal assistance mechanism should be more efficient and effective.

[20] European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, Brussels, 12 July 2016.

[21] Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2 June 2016.

In such scenario, strengthening the mutual legal assistance procedures, such as collecting e-evidence, using the Budapest Convention, is not a solution if not address the territoriality principle. As pointed by the Council, close cooperation with internet service providers should be promoted. Further, EU generally adopted a soft integration for criminal matters, based on the mutual recognition principle and build on minimum standards, rather than harmonization. However, member-states procedures in the fight against organized crime consistently differ and having in mind the cross-border dimension of these crime activities, member-states failed effectively to cooperate.

As long as the EU cooperation is strengthening in its internal borders, EU could not deny its own external dimension. EU should put forward a concrete frame for further facilitation of investigation, especially in cross-border cases when evidences are held by US communication providers. Following the European security agenda and the Council conclusions, EU should start implementing such partnership. This framework should be built on pan-EU harmonized instrument which enables direct contacts between law enforcement from one jurisdiction and service providers from another.

4. Case studies on e-evidence: France, Germany and Italy

Terrorist attacks in Europe influenced the change of thinking regarding cybercrime, especially in Germany, France and Italy. These states started empowering their national security and law enforcement authorities with tools for effective investigations of organized crime and terrorism in cyberspace.

The terrorist attacks changed the security and legislative landscape in France, where the emergency state is still in force. The new Antiterrorism law is adopted in July 2016 and anticipates new simplified conditions from computer seizure to the level of considering the balance between security and civil rights.[22] Although, mainly considered as prevention of terrorism, the computer seizure is allowed for targeting individuals that represent threat for national security. In Germany, new version of Remote Communication Interception Software was approved by the Ministry of Interior in 2016 and new antiterrorism law is adopted in August 2016, expanding the competences of law enforcement and intelligence agencies.[23] The software takes the surveillance of communications one step further and enables monitoring computer communications and other electronic devices before communications and data are encrypted. The software is legally limited to the interception of real-time

[22] Law No. 2016-987 of 21 July 2016, https://www.legifrance.gouv.fr/affichTexte.do?cid Texte=JORFTEXT000032921910

[23] Germany, Act to improve anti-terror information exchange in force, 26 July 2016.

communication, messaging software, as well as email conversations. Moreover, the Ministry of Interior is planning to establish a new agency focused on the decryption of communications.[24] In Italy, the encryption and the introduction of Trojan horses for interception of communications in the Criminal Procedure Code animated parliamentary discussions and public debates on the possibility of exploiting these new instruments to prosecute criminals in cyberspace.[25]

France, Germany and Italy have similar legislative framework which determines how the investigations are conducted in cyberspace. These are privacy data protection laws, criminal laws, data retention policies and electronic communication laws. Also, these states have privacy protection laws and data control and limitations how private data and other information are transferred to public or private organizations. The level of data protection in France is considered to be highly enough; in Germany privacy is protected by the Constitution and the Federal Data Protection Act[26]; the Italian Privacy Law is an important legislation that intervenes in order to assess the effects of new potential harmful provisions on citizen's privacy.[27]

Regulations and procedures that govern how e-evidences are collected and used in trials are evident in different criminal and criminal procedure laws. Still, some elements need to be indicated: these states lack of proper definition on e-evidence; while the German and French law puts in details the use of malwares in criminal investigations, the Italian criminal procedure law makes no such reference; there are some commonalities across legislations regarding the fight against cybercrime and references on integrity and data originality, emerging from the Budapest Convention.

These states also have data retention policies whose conditions vary more or less significantly. In France, data retention is predicted for a period of one year.[28] In Germany, a new data retention law entered in force in October 2015 and forced providers to return traffic data in period up to 10 weeks.[29] In Italy, a new law obligates

[24] German Ministry of the Interior, Zwei Jahre Digitale Agenda der Bundesregierung, 7 September 2016.

[25] Codice di procedura penale, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della. repubblica:1988-09-22;447.

[26] Federal Data Protection Act, https://www.gesetze-im-internet.de/englisch_bdsg.

[27] Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4814258.

[28] Code des postes et des communications electroniques, http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPOSTE.rcv.

[29] Germany, Act introducing a storage obligation and a maximum retention period for traffic data, 10 December 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf.

providers to return all telephone and electronic communications traffic data until June 2017.[30]

What it needs to be noticed from such designated legislation is the existence of uncertainties regarding who should be subject to it and whether legislation is being effectively enforced. Although the French law forces domestic internet service providers to return data in order to confront with criminal investigations, the French justice allowed national authorities to send formal requests to international service providers. In Germany, domestic and international service providers must cooperate with national authorities; if the provider refuses, it may be fined up to 100.000 euro. It is important to stress out that the data retention policies are provisions in the electronic communication laws of France and Germany, therefore the insecurity created by the absence of proper definition also reflects on data retention policies. In Italy, according the Electronic Communication Law, those authorized to secure connection or electronic communication services are bound to cooperate with national authorities and to secure compulsory services, including interception of communications.[31]

Relations with the USA are main concern. French National Assembly voted for two international conventions in January 2016 on mutual legal assistance in criminal matters.[32] These conventions are conceived to include the consequences of the digital technologies use in criminal offences and to ease the access to information for criminal pursuit by authorities of both states. According such framework, the collected information should be stored only during the investigation stage and national authorities must hand over any mistakes in data handling. Finally, both sides might refuse transfer of information if endangers the national security and sovereignty. Germany and Italy have not signed agreements with the USA based on the recent terroristic attacks and no such perspective could be seen in the future. They rely on mutual legal assistance agreements signed back in 2006 for exchange of e-evidence between national authorities.

[30] Legislative Decree No. 196 of 30 June 2003, supplemented by Law No. 21 of 25 February 2016.

[31] Legislative Decree No. 259 of 1 August 2003 (Codice delle comunicazioni elettroniche), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259.

[32] French National Assembly, judiciaires, 28 January 2016, http://www.assemblee-nationale.fr/14/cri/2015-2016/20160113.asp.

Conclusion

EU put forward a series of instruments for strengthening the judicial cooperation in criminal matters. In this sense, the mutual recognition principle is a basic instigator of judicial cooperation and advantages rely on mutual trust of legal systems for speedily enforcement of judicial decisions. For purposes of securing and acquiring e-evidence, the EIO is a significant step in two fronts; first, it creates a harmonized instrument regulating the collection and exchange of evidence, including data from interceptions; second, it represents a significant guide for development of the mutual recognition principle, although not in every cross-border scenario in which interception could be necessary.

EU's attempt to systematize collection of evidence may not deliver the complete harmonization of collection and exchange of e-evidence in crime investigations. Investigative powers and rules of criminal procedure, even among states with similar legal systems, may differ from state to state. Therefore, it may happen that the e-evidence, acquired according the rules of one legal system not to be appropriate to create reliable ground for decision-making in other legal system. With no comprehensive legal frame, defying specific standards for procedures and modalities for collection and exchange of e-evidence, member-states tend to act differently, mostly on case by case. Thus, acquiring electronic evidence remains governed by national law and national criminal procedure.

In such complex image, the 2001 Convention on Cybercrime remains leading international and legal frame for prosecuting cybercrime. With its provisions which enable expeditiously actions, the Convention in some cases may offer rapid and efficient regime or international criminal justice, thus responding to the collection of e-evidence issue. Undoubtedly, the Budapest Convention, which enables authorities to secure computer data in specific criminal investigations, contributed for strengthening the cooperation in the fight against cybercrime. However, the Convention remains limited in its extent, as it applies only on evidence leading towards conviction of computer related crime. Further, relying mostly on mutual legal assistance, instead on mutual recognition or direct trans-border access, it is criticized for general non-efficiency and especially obtaining e-evidence. Therefore, e-evidence collection in cyberspace is still dependant on voluntary cooperation among authorities or on complicated procedures for mutual legal assistance.

On EU-US cooperation overall, procedures are long because on the European side, it is not always easy for national authorities to write requests that will fulfil US legal standards; on the USA side, it seems that US authorities are overflowed with requests to their service providers for producing e-evidence, sent not only from France, Germany or Italy, but from most of the EU member-states. Further, some kind of direct or voluntary cooperation between national authorities and some US providers exists, but it seems limited only on exchange of generic subscriber data.

Germany and Italy would like to see institutionalization of more constructive and efficient cooperation with service providers.

At the same time, the judicial cooperation between EU and USA should not be ignored, as the data flow will increase through the Atlantic for commercial and security purposes in the years to come. Recent events with the Snowden affair inevitably shaken the digital relations between EU and USA and increased the public awareness on how the authorities and intelligence services should have access to data. Regarding what is already in force or needs to be approved, improved mechanisms are necessary between the EU and the USA for continuing the cross-border request of data.

EU member-states – France, Germany and Italy – share significant legislation which is vital for judicial cooperation in criminal matters. Further, the Budapest Convention, which is not EU legislation, but is ratified by 25 member-states adds additional layer of commonality. A joint Franco-German declaration from August 2016 offers some other insights of possible ways for strengthening the judicial cooperation and eventual EU level harmonization.[33] Besides the identification of solutions for pursuing suspicious terrorists who communicate by encrypted means, Ministers of interior of France and Germany call on the European Commission to propose new legislation that would force communication and internet providers to cooperate with judicial authorities of the state where they offer its services.

There is a large part of common characteristics among EU member-states. From the enhanced investigative techniques and similar national legislation frameworks governing the collection of e-evidence to the significance of the judicial cooperation with the USA and service providers, at EU level there is a solid ground for common approach but it is far from being definite. Rules regarding collection and exchange of e-evidence in EU and between member-states and third states still rely on complicated mutual legal assistance agreements. In this regard, authorities in France, Germany and Italy agree on the need of processes at EU level for enabling effective cyberspace investigations. This could be preferred by the member-state's attempts to empower their investigation powers with extraterritorial effect, potentially putting overseas and multination providers in difficult jurisdictional situation. Harmonized, multinational agreement on the scope of powers and minimal protection, shall secure clear and transparent action area.

Once guidelines are clearly set, every single actor must do its share and play according the same rules. The trust among law enforcement agencies, judicial authorities, users, civil society, service providers and EU institutions must complete the process. All parties must acknowledge that this kind of trust is heavy to build, but

[33] German Ministry of the Interior and French Ministry of the Interior, 23 August 2016, http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiativefranco-allemande-sur-la-securite-interieure-en-Europe.

easy for destruction. Rejecting the needs of different interested parties may only increase the conflict and instead of antagonizing the "private vs. security", all actors must dedicate on clear frameworks and to work together on their application.

REFERENCES

Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2 June 2016.

Agreement on Mutual Legal Assistance between the European Union and the United States of America, Washington, 25 June 2003.

Code des postes et des communications electroniques, http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPOSTE.rcv.

Codice di procedura penale, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della. repubblica:1988-09-22;447.

Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America OJ L 291, November 7, 2009.

Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001.

Council of Europe, The European Convention on Mutual Assistance in Criminal Matters, Strasbourg, 20 April 1959.

Council of the EU, Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member states of the European Union, OJ C 197, July 12, 2000.

Council of the EU, Council Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9 June 2016.

Council of the EU, Council Decision Concerning the Definition of the Schengen Acquis, 20 May 1999, OJ L 176, July 10, 1999.

Council of the EU, Council Framework Decision 2002/584/JHA on the European Arrest Warrant, Brussels, 13 June 2002, OJ L 190, July 18, 2002.

Council of the EU, Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence, 22 July 2003, OJ L 196/45, August 2, 2003.

Council of the EU, Council Framework Decision 2008/978/JHA on the European Evidence Warrant, 18 December 2008, OJ L 350/72, December 30, 2008.

Council of the EU, Declaration on Combating Terrorism, Brussels, 25 March 2004.

Council of the EU, The Schengen Acquis Integrated in the European Union, OJ L 239/1, September 22, 2000.

Court of Justice of the EU, Judgement of the Court in Joined Cases C-293/12 and C-594/12.

Directive 2016/680 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/1, May 4, 2016.

Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201/37, July 31, 2002.

Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, OJ L 105/54, April 13, 2006.

Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130/1, May 1, 2014.

European Commission, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows, Brussels, 12 July 2016.

European Commission, Mutual Recognition of Final Decisions in Criminal Matters (COM/2000/495), 26 July 2000.

European Commission, The European Agenda on Security, COM(2015) 185 final, Strasbourg, April 28, 2015.

Federal Data Protection Act, https://www.gesetze-im-internet.de/englisch_bdsg.

French National Assembly, 28 January 2016, http://www.assemblee-nationale.fr/14/cri/2015-2016/20160113.asp.

German Ministry of the Interior and French Ministry of the Interior, 23 August 2016, http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiativefranco-allemande-sur-la-securite-interieure-en-Europe.

German Ministry of the Interior, Zwei Jahre Digitale Agenda der Bundesregierung, 7 September 2016.

Germany, Act to improve anti-terror information exchange in force, 26 July 2016.

Germany, Act introducing a storage obligation and a maximum retention period for traffic data, 10 December 2015, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf.

Law No. 2016-987 of 21 July 2016, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032921910

Legislative Decree No. 196 of 30 June 2003 (Personal Data Protection Code), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4814258, supplemented by Law No. 21 of 25 February 2016.

Legislative Decree No. 259 of 1 August 2003 (Codice delle comunicazioni elettroniche), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259.

Regulation 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and repealing Directive 95/46/EC, OJ L 119/1, May 4, 2016.