IAI
Istituto Affari Internazionali

ISSN 2280-6164

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace

edited by Tommaso De Zan and Simona Autolitano

ABSTRACT

In today's ultra-connected world, much of our life occurs online. From watching TV series on Netflix, buying discounted airplane tickets on Kayak, to chatting with an old friend living in another continent on Facebook, it is hard to imagine a "disconnected" life. Despite the benefits generated by increased connectivity and more powerful processing tools, ICT systems have not only been employed to foster social and economic development. Terrorists and cybercriminals are increasingly using cyberspace to conduct their malfeasances. In June 2016, the Council of the European Union underlined the importance of improving the effectiveness of criminal justice in cyberspace. Using the Council conclusions as a starting point, the paper provides some "policy suggestions" for the ongoing debate taking place within EU institutions. In order to do so, the paper seeks to answer three main questions: What are the main challenges that EU member states face today when they collect e-evidence? How are they tackling these issues? Can an EU common framework provide solutions to solve these problems?

This study has been conducted with the support of Microsoft. The analysis and opinions expressed herein are solely those of the authors.

keywords

Cyber-security | France | Germany | Italy | International law | EU law | European Union | USA | Transatlantic relations

EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace

edited by Tommaso De Zan and Simona Autolitano*

* Tommaso De Zan is junior researcher at the Istituto Affari Internazionali (IAI). Simona Autolitano is intern at IAI.

· Paper prepared for the Istituto Affari Internazionali (IAI), November 2016. Presented at the seminar "EUNITED against Crime: Digital Evidence, Privacy and Security in the European Union" held in Brussels on 23 November 2016, organized by the Centre for European Policy Studies (CEPS) and IAI. This study has been conducted with the support of Microsoft. The analysis and opinions expressed herein are solely those of the authors.

ISSN 2280-6164
DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

Preface

Since 2015, the terrorist attacks in France and Belgium have become synonymous with an increased security threat, influencing the public debate and leading EU and member states' authorities to propose several measures aimed at tackling the issue of increased protection. The problems vying for attention in political agendas are piling up, from the growth of populist political forces to problems linked to immigration. Among these, the priority given to the fight against terrorism has stressed some specific issues. With criminal activities increasingly moving across borders, the problem of retrieval and use of data on an international basis for crime prevention and investigation of criminal actors has come to the fore. The issue has moved beyond "classical" borders to digital ones, as the "digital dimension" of criminal activity grows. Investigations into "anti-terrorism" are, for example, increasingly concentrating on terrorists' online activities.

The Istituto Affari Internazionali (IAI) has a long tradition in security studies. This includes a new focus on research that looks into the nexus between security and technology with several recent papers launched under the coordination of Jean-Pierre Darnis, Head of IAI's Security and Defence Programme. This technological focus is an opportunity for renewed analysis and dialogue with the extended community of stakeholders, from technology producers to security institutions. Space policy, cyber security and new technological security agendas, are among the fields scrutinized by our researchers, often within European research consortiums.

This specific interest in the relation between technology and security has led us to deepen our analysis of the correspondence between crime and cyber domains. This is the starting point of the IAI report "EUnited against crime: improving criminal justice in the European Union's cyberspace" authored by Tommaso de Zan and Simona Autolitano.

As a starting point, the authors have taken into consideration relevant national case studies such as France, Germany and Italy to deepen our understanding of online privacy and the fight against terrorist and criminal activities in each country. The issues of e-evidence and of access to and use of digital information by judicial and police forces for trials are among key points.

The first important problem to arise is that of cross border data requests for e-evidence. This apparently simple technical issue triggers a series of problems directly related to sovereignty and the rule of law in the digital age.

Some key elements from the IAI report can be highlighted. First of all, as certain criminal activities are deeply rooted in cyberspace, there is a compelling need for countries' national authorities to counteract this type of crime. However, it is often difficult to understand whose jurisdiction should be applied, and this is

ISSN 2280-6164

particularly true for service providers that might be based in a country while having their data stored in another. Secondly, there is significant room for improvement in the international framework. As the study illustrates, the European Union is undergoing an important evolution: a common EU approach is undoubtedly the most appropriate solution compared to the patchwork of member states' legislation and bilateral frameworks, which are rapidly being overcome by the complexity of criminal digital activities and by the different ownership of IT infrastructures. However, a common EU approach is not enough as the US plays a leading role in the IT industry, with a unique concentration of company ownership, research, investment and a massive market. This is the reason why this study advocates for an EU harmonized approach as well as for a renewed transatlantic partnership in order to cope with crime in the digital age.

The study therefore carries an important political message. In a globalized era, upholding the rule of law requires a multilateral framework among democracies. This is a strong case both for the deepening of the EU's regulatory aspects as well as for international agreements between the EU and third countries, mainly, although not exclusively, with the US. It is paradoxical to note that in difficult times, while terrorists, criminals and populist forces threaten Europe, important issues can often be solved through a deeper integration. However, following terrorist attacks, governments' first moves usually involve raising fences, for example with the re-establishment of controls within the Schengen area. Yet, if we want to seriously tackle cross-border crime and terrorism, we need to improve our cooperative multilateral frameworks instead of concentrating on national approaches, which can be too slow and inadequate for the task. The conundrum governments face, is to solve problems that call for an integrated and harmonized approach while public opinion demands symbolic national action to be taken. There is hope that information technology, by its very nature, has fostered the development of a cross-border sense of community among the younger generations, a different approach to internationalism compared to the ideological trends of the past. This represents a new frontier, a unified world that needs to ensure "digital protection" in a time of cybercrime and terrorist use of cyberspace. It is also a sign of the renewed interest for analysis and policy proposals from a think tank such as IAI, with a long tradition of cross-border European and transatlantic studies.

Ferdinando Nelli Feroci
President of the Istituto Affari Internazionali

ISSN 2280-6164

Executive summary

In today's ultra-connected world, it is not bold to claim that much of our life occurs online. From watching TV series on Netflix, buying discounted airplane tickets on Kayak, to chatting with an old friend living in another continent on Facebook, it is hard to imagine a "disconnected" life. Despite the benefits generated by increased connectivity and more powerful processing tools, ICT systems have not only been employed to foster social and economic development: cybercrime is on the rise and the value of its economic damage is projected to reach 2 trillion dollars by 2019; terrorist organizations are steadily employing cyberspace to recruit new adepts, spread their propaganda, trigger the treacherous actions of lone wolves and attack "infidels'" critical infrastructures; even traditional organized crime groups, like the Italian Mafia, are now moving their operations to the web.

In this context, law enforcement authorities should be fully equipped to effectively conduct investigations to prevent, detect and prosecute organized crime and terrorist groups using ICTs. Nonetheless, because of the borderless nature of internet, data that can be used as proof of culpability in court (the so-called e-evidence) is not always within the immediate reach of national law enforcement authorities. Data can be stored where the headquarters of a service provider is located or even moved across different countries. Therefore, international judicial cooperation should be consolidated to allow national authorities to obtain data when it is found or moves across jurisdictions. Last but not least, privacy should continue to be protected and citizens should not fear that their online data are indiscriminately accessed by government authorities regardless (or in the absence) of proper legal safeguards.

In June 2016, the Council of the European Union underlined the importance of improving the effectiveness of criminal justice in cyberspace. By departing from the Council conclusions, the primary scope of this paper is to feed some "policy suggestions" into the ongoing debate taking place within EU institutions. In order to do so, this paper seeks to answer three main questions: What are the main challenges that EU member states face today when they collect e-evidence? How are they tackling these issues? Can an EU common framework provide solutions to solve these problems?

The description of the procedures and challenges related to the collection of e-evidence within and outside the jurisdiction of the selected EU member states, namely France, Germany and Italy, sheds light on some important commonalities and differences that need to be kept in mind. Four macro elements seem of major relevance: (1) the impact on national legislation and investigative techniques of the recent terrorist attacks in Europe; (2) although different in content and nature, similar legislative frameworks determining how e-evidence should be collected; (3) the importance of judicial cooperation with the United States and American service

ISSN 2280-6164
DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

providers; (4) the European Union as a common denominator and the related gaps in the Union's legislation concerning e-evidence. In spite of the limited number of selected countries, this analysis reveals a great deal of common traits between them. From the cause of renewed enhanced investigative techniques, namely terrorism, and similar national legislative frameworks governing the collection of e-evidence, to the importance of judicial cooperation with the USA and US based service providers, room for a common approach at the EU level exists. Nonetheless, the EU normative framework is far from being definitive. Rules pertaining to the collection and exchange of e-evidence within the EU and between EU member states and foreign countries are still relying on rather cumbersome MLAT processes. In this respect, in all three countries, officials and experts agree on the necessity of stirring an EU level process to enable effective investigations in cyberspace. This might be preferable to member states' attempts to give their investigative powers extraterritorial effect, potentially putting overseas or multinational providers into difficult jurisdictional situations. A harmonized, multinational accord on the scope of powers, and minimum protections, would ensure a clear, transparent and level playing field.

This report proposes some "policy suggestions" to the issues delineated by the Council in its June 2016 conclusions. The subject-oriented approach should determine which country can be the "investigating state;" however, it is the country of habitual residence of the person whose data are sought that should have the authority to send a "production order" for the disclosure of data to the relevant service provider. Since it is offering its services there, the receiving service provider should then abide by the law of the country sending the production order. To make this work, a series of inevitable actions should follow. The EU should adopt a common framework clearly defining "e-evidence," what is a "service provider" and what it means to be "offering services in the EU." To make judicial cooperation more efficient, the EU should make clear the application of the principle of mutual recognition enshrined in the EIO to e-evidence. Yet, all these much-needed reforms would be of little help, if legislation change were not pursued in relevant third countries. Having ascertained the predominant role of the USA and of US based service providers, the EU should sign a cross-border data request agreement with the US Government. The agreement should make sure that relevant American legislation, namely ECPA, is changed to allow US service providers to disclose data to EU authorities, when these can legally send a production order. The reverse should be made possible too. Such an agreement is feasible given EU high standards in data protection and human rights, and would probably be welcomed in the USA as well, where policymakers are advancing solutions (such as ICPA) going in the same direction. The transatlantic framework would be reinforced and the lingering paradox of imposing US criminal law upon EU criminal cases will be dispelled. The report suggests also other measures, including a common EU-USA data retention regime, an enhanced role for Europol and Eurojust and the establishment of specific mechanisms regulating how service providers should handle production orders.

ISSN 2280-6164

The proposed policy suggestions do not offer all answers, but might be a good place to start. If adopted, and in the context of crime investigation, they will not require any forced data localization policy in Europe or elsewhere by states eager to control access to citizens' data; it will not make it necessary to resort to international hacking, if not in extreme cases and until the residence of the person whose data are sought is known; it will make decryption tools useless, as data will be made available by direct contact with service providers, when legal requirements are met; it will provide much clarity for service providers, which will not have to choose between the lesser of two evils when confronting different jurisdictional claims; citizens' privacy will be upheld.

Once clear guidelines are established, every single actor in the game must do his part and play according to the same rules. Trust between law enforcement agencies, judicial authorities, users, civil society advocates, service providers, EU and USA institutions should permeate the process. Nonetheless, stakeholders should recognize that this kind of trust is hard to build but easy to elapse, and continuous revelations about opaque programmes do not necessarily inspire such a sentiment. Snubbing the various stakeholders' needs will only exacerbate conflict and, instead of antagonizing imaginary "privacy vs security" groups, all actors should commit themselves to clear frameworks and work together to make them function.

ISSN 2280-6164

Introduction

Background and research questions

In today's ultra-connected world, it is not bold to claim that much of our life occurs online. From watching TV series on Netflix, buying discounted airplane tickets on Kayak, to chatting with an old friend living in another continent on Facebook, it is hard to imagine a "disconnected life." Modern digital information and information communication technologies (ICT) are the main drivers behind the so-called "Information Society," a society in which the creation, distribution, use, integration and manipulation of information is a significant economic, political, and cultural activity.[1] Despite the benefits generated by increased connectivity and more powerful processing tools, ICT systems have not only been employed to foster social and economic development: cybercrime is on the rise and the value of its economic damage is projected to reach 2 trillion dollars by 2019;[2] terrorist organizations are steadily employing cyberspace to recruit new adepts, spread their propaganda, trigger the treacherous actions of lone wolves and attack "infidels" critical infrastructures;[3] even traditional organized crime groups, like the Italian Mafia, are now moving their operations to the web.[4] Against this backdrop, the collection of electronic evidence (e-evidence) – defined for the purpose of this paper as "data (comprising the output of analogue devices or data in digital format) 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 process of adjudication" – is becoming more and more relevant in criminal justice to successfully prosecute not only cybercrime but all criminal offences.[5]

In June 2016, the Council of the European Union underlined the importance of improving the effectiveness of criminal justice in cyberspace.[6] The Council concluded that such an improvement should occur through enhanced cooperation with service providers, reorganization of mutual legal assistance (MLA) proceedings, and review of the rules to enforce jurisdiction in cyberspace.

[1] Claudia Sarrocco, *Elements and Principles of the Information Society*, ITU background paper for the World Summit on the Information Society (WSIS), 25 August 2002, http://www.itu.int/osg/spu/wsis-themes/access/index.html.

[2] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", in *Forbes*, 17 January 2016, http://onforb.es/1P91xQy.

[3] Gabriel Weimann, *Terrorism in Cyberspace. The Next Generation*, Washington, Woodrow Wilson Center Press/New York, Columbia University Press, 2015.

[4] Raffaella Natale, "Cybercrime: la mafia s'è spostata sul web. Per l'Interpol costa all'Europa 750 miliardi l'anno", in *Key4biz*, 9 May 2012, https://www.key4biz.it/?p=25291.

[5] See Stephen Mason, *Electronic Evidence. Disclosure, Discovery and Admissibility*, London, Butterworths, 2007, par. 2.03.

[6] Council of the European Union, *Council Conclusions on Improving Criminal Justice in Cyberspace*, Luxembourg, 9 June 2016, http://europa.eu/!XX67Kg.

ISSN 2280-6164

By departing from the Council conclusions, the primary scope of this paper is to feed some "policy suggestions" into the ongoing debate taking place within EU institutions. In order to do so, this paper seeks to answer three main questions: What are the main challenges that EU member states face today when they collect e-evidence? How are they tackling these issues? Can an EU common framework provide solutions to solve these problems?

To answer these questions, this paper is organized as follows. Sections 1, 2 and 3 describe and analyze the main challenges the national authorities of France, Germany and Italy face when they collect e-evidence within and outside their jurisdiction and how they are coming to grips with these issues. A set of common topics and questions was developed to allow cross-country comparisons: the three cases studies look into member states' 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.[7] Every case study specifically addresses judicial relations with the USA as it is the country to which member states send the vast majority of their cross-border data requests. The scope of these sections is to gain further insights on the causes that are contributing to make the collection of e-evidence such a daunting task and have a preliminary understanding of possible policy responses. Section 4 is dedicated to detailing the current EU legislative framework on criminal justice cooperation and to understand whether this facilitates or not collaboration between member states and between member states and the USA. Section 5 first provides an analysis of the main commonalities and differences that can be found in the acquisition of e-evidence in the three selected countries in the broader EU context. This analysis then paves the way for a series of policy suggestions to improve EU criminal justice in cyberspace.

Further focus: Why improving criminal justice in cyberspace is important?

In the context of the fight against crime, *law enforcement authorities should be fully equipped to effectively conduct investigations to prevent, detect and prosecute organized crime and terrorist groups using ICTs*. As European Commission President Jean-Claude Juncker states in his guidelines "combating cross-border crime and terrorism is a common European responsibility," as no single country is able to tackle today's complex problems on its own.[8] In April

[7] For the purpose of this report, unless otherwise specified, service provider is defined as: "any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service." See Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, Strasbourg, Council of Europe, 16 September 2016, p. 18, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

[8] Jean-Claude Junker, *A New Start for Europe. My Agenda for Jobs, Growth, Fairness and Democratic Change. Political Guidelines for the next European Commission*, Strasbourg, 15 July 2014, http://europa.eu/!vu77nf.

ISSN 2280-6164

2015, the European Agenda on Security set three main security priorities for the EU: terrorism, organized crime and cybercrime.[9] To investigate crime, competent judicial authorities should be able to enforce jurisdiction in cyberspace and obtain the evidence and information they require. As also recently highlighted in the Agenda's first progress report,[10] an effective fight against terrorism and organized crime should be adaptable to the new trends in criminality and their increased use of cyber-means. The urgent need for a more effective European police and judicial cooperation in criminal matters was made even more evident after terrorists struck Europe's heart in Paris and Brussels. Both conducted by Islamic State of Iraq and Greater Syria (ISIS) affiliates, the two murderous attacks in November 2015 and March 2016 claimed the life of more than 160 and injured approximately 500 European citizens. In this context of "crumbling security," the joint declaration by France and Germany of August 2016 has stressed, once again, the need to enhance security in Europe through effective cyberspace investigations.[11]

However, because of the borderless nature of internet, data that can be used as proof of culpability in court is not always within the immediate reach of national law enforcement authorities. These data can be stored where the headquarters of a service provider is located or even moved across different countries. Therefore, *international judicial cooperation should also be consolidated to allow national authorities to obtain data when it is found or moves across jurisdictions*.[12] However, the current international framework, if not entirely broken, is not proving to be working effectively. Mutual legal assistance (MLA) in the form of Mutual Legal Assistance Treaties (MLATs) should be the most common solution for law enforcement authorities to gather cross border e-evidence.[13] Such a procedure

[9] European Commission, *The European Agenda on Security* (COM/2015/185), 28 April 2016, p. 2, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52015DC0185.

[10] European Commission, *First Progress Report towards an Effective and Genuine Security Union* (COM/2016/670), 12 October 2016, p. 5, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52016DC0670.

[11] German Ministry of the Interior and French Ministry of the Interior, *Initiative franco-allemande sur les enjeux clés de la coopération européenne dans le domaine de la sécurité intérieure*, 23 August 2016, http://www.interieur.gouv.fr/Le-ministre/Interventions-du-ministre/Initiative-franco-allemande-sur-la-securite-interieure-en-Europe.

[12] Fort the purpose of this paper we refer to: (1) Subscriber information/data: "any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a) the type of communication service used, the technical provisions taken thereto and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement." (2) Traffic data: "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." (3) Content data: everything that is not subscriber or traffic data. The two definitions of subscriber and traffic are those of articles 1 and 18 of the Budapest Convention. See Council of Europe, *Convention on Cybercrime*, Budapest, 23 November 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[13] MLATs are international agreement that, generally, sets out a specific list of agreed crime and

ISSN 2280-6164

rests on the recognition of countries' territorial sovereignty, which requires formal consent of the country where data are located. Nevertheless, for the purpose of collecting e-evidence, the traditional cooperation based on MLATs is turning out to be increasingly problematic. Procedures could take various months due to bureaucratic hurdles,[14] while legal requirements such as dual criminality[15] and the absence of arrangements for expeditious actions critically hamper judicial cooperation. Consequently, MLA mechanisms are often inefficient to secure volatile evidence in unknown or multiple jurisdictions, and therefore prompt practitioners to resort to other means to lock down evidence when needed. Moreover, as MLATs are based on the principle of territoriality, relying on these mechanisms could be even more troublesome if the actual location of digital data is unknown.[16] When data are stored using cloud technology,[17] the issue of location becomes more involved: even indicating which data are stored where is potentially harmful, thus making it really difficult to ascertain which country the request of data disclosure should be addressed to.[18] Determining the location of data is further complicated when criminals use specific software to hide or dissimulate their IP addresses. Hence, despite the fact that much of e-evidence could now be "anywhere in the cloud" and in spite of easier ways for criminals to effectively conceal their malfeasances, international cooperation is still grounded on cumbersome MLA processes, which are ill-suited to deny criminals a safe haven in cyberspace.

To avoid entangling themselves in exhausting procedures to obtain e-evidence, national authorities have increasingly demanded service providers be more "cooperative" in their fight against crime and serious threats. In some instances, law enforcement authorities and providers have struck agreements or informal

provisions aiming to foster international judicial cooperation, including the collection of evidence, for those specific crimes. For an overview on worldwide MLATs see: https://mlat.info.

[14] Joshua I. James and Pavel Gladyshev, "A Survey of Mutual Legal Assistance Involving E-Evidence", in *Digital Investigation*, Vol. 18 (June 2016), p. 23-32, http://fulltext.study/preview/pdf/457999.pdf.

[15] The requirement of "dual criminality" implies that an offense shall be an extraditable offense if it is considered criminal under the laws of both the surrendering and requesting nations.

[16] MLA procedures relies on the recognition of territorial sovereignty of one's state territory. According to international law, the exercise of jurisdiction to enforce on the territory of another State is permitted only if the latter provides consent. See Permanent Court of International Justice, Judgement of 7 September 1927 in *The Case of the S.S. "Lotus"*, PCIJ Series A, No. 10, http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[17] Cloud computing is an internet-based infrastructure, which provides users and enterprises with various capabilities to store and process their data in third-party data centre, which might be located anywhere in the world. It enables "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". See Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing", in *NIST Special Publications*, No. 800-145 (September 2011), p. 2, http://dx.doi.org/10.6028/NIST.SP.800-145; Frank Alleweldt et al., *Cloud Computing*, Brussels, European Parliament, May 2012, p. 5, http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL-IMCO_ET(2012)475104.

[18] Alexander Seger, "Evidence in the Cloud and the Rule of Law in Cyberspace", in *Europe's World*, 7 December 2015, http://europesworld.org/?p=10119.

ISSN 2280-6164

arrangements, especially in relation to less "intrusive kind of data," to exchange e-evidence in the context of crime investigations.[19] However, service providers are often caught between two fires. Especially for those offering services in multiple countries, complying with one state's legislation might infringe the law of the country where their headquarters are located or where the data are stored. The case of the Microsoft executive who was arrested in Brazil for not handing over content data of a Brazilian's Skype calls stored in the USA, as doing so would have produced a felony in the USA, is indicative of the traps of the current incongruous international framework.[20] From such a scenario derives a great degree of uncertainty: on one hand, law enforcement authorities winsomely welcome providers' collaboration, but they are baffled when providers refuse to hand over the data that are most precious to solve a criminal case; on the other hand, service providers seem to be eager to cooperate, but they are frustrated in facing the unintended consequences of their collaborative actions when they offer their services in different jurisdictions.

The instability generated by the absence of a comprehensive solution is further worsened when single national laws or courts' decisions "unilaterally" take aim at these problems, while not fully realizing the international implications of their actions.[21] In the Yahoo! Inc case, the Belgian Supreme Court ruled against the American company, arguing that since Yahoo! is "virtually" located in Belgium when it offers its communications services, it should comply with Belgian law regardless of the location of its headquarters or the actual location of its data. Henceforth, Yahoo! will have to disclose data to Belgian law enforcement agencies upon request.[22] Someone referred to this decision as the "end of international assistance in criminal matters."[23] On the other side of the Atlantic, instead, the United States Court of Appeals has ruled that courts are not authorized "to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers."[24] Relevant authors

[19] Cybercrime Convention Committee, *Criminal Justice Access to Data in the Cloud: Cooperation with "Foreign" Service Providers, Council of Europe*, Strasbourg, 3 May 2016, p. 21, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d.

[20] Dina Bass, "The Case That Has Microsoft, Apple and Amazon Agreeing for Once", in *Bloomberg*, 2 September 2015, http://bloom.bg/1XeUIyj.

[21] Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, Tallin, NATO Cooperative Cyber Defence Centre of Excellence, 2015, https://ccdcoe.org/node/732.html.

[22] Nicolas Roland, "Court of Appeal of Antwerp Confirms Yahoo!'S Obligation to Cooperate with Law Enforcement Agencies", in *Stibbe News & Insights*, 15 July 2014, http://www.stibbe.com/en/news/2014/july/court-of-appeal-of-antwerp-confirms-yahoos-obligation-to-cooperate-with-law-enforcement-agencies.

[23] Steven De Schrijver and Thomas Daenens, "The Yahoo! Case: The End of International Legal Assistance In Criminal Matters", in *Who'sWhoLegal*, September 2013, http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters.

[24] US Court of Appeals for the Second Circuit, *Opinion in the case Microsoft v. United States*, Docket No. 14-2985, 14 July 2016, p. 2, http://www.ca2.uscourts.gov/decisions/isysquery/6a195bc9-a594-42ab-99d0-56a20bab3996/1/doc/14-2985_complete_opn.pdf.

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016 ISSN 2280-6164

have been quick to point out the "dangerous implications" of the case.[25] Similarly, and to reiterate how widespread these issues are, on 11 August 2016, the Pakistani Parliament adopted the "Prevention of Electronic Crimes Act"[26] consenting authorized officers to "have access to and inspect the operation of any specified information system," so to investigate any act committed outside Pakistan against the country and every citizen of Pakistan wherever it may be (art. 32).

Instead, audacious international frameworks might be secured, as previous important conventions and agreements have shown. A notable example is the 2001 Budapest Convention, which pursues "a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation."[27] A more recent example is the agreement signed in July 2016 on cross-border data requests between the United Kingdom and the United States,[28] which some experts have urged privacy rights advocates to embrace.[29]

Despite being fraught with pitfalls and hurdles, carefully designed international frameworks might therefore be the best path to follow, instead of adopting domestic measures that, desynchronized from a commonly accepted solution, run the risk of leading to a "free-for-all situation," where countries assertively try to reach an elusive kind of justice on their own.

Last but not least, *privacy should continue to be protected and citizens should not fear that their online data are indiscriminately accessed by government authorities regardless (or in the absence) 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, revelations of the National Security Agency's (NSA) activities brought to the surface by American whistleblower Edward Snowden have much influenced ongoing discussions on the importance of ensuring privacy in cyberspace.[30] While, as we said earlier, law enforcement agencies need to have the technological and legal instruments to guarantee the safety and security of citizens, access to data should occur in the context of crime investigations and under the safeguards and legal requirements of countries' criminal procedure laws. Arbitrary

[25] Jennifer Daskal, "The Dangerous Implications of the Microsoft Ireland Case", in *Just Security*, 14 October 2016, https://www.justsecurity.org/33577.

[26] National Assembly of Pakistan, *Prevention of Electronic Crimes Act*, 11 August 2016, http://www.na.gov.pk/uploads/documents/1470910659_707.pdf.

[27] See Preamble: Council of Europe, *Convention on Cybercrime*, cit.

[28] US Department of Justice, *Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combating Serious Crime Including Terrorism*, 15 July 2016, https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf.

[29] Jennifer Daskal, "To Privacy Rights Advocates: Embrace DOJ's Cross-Border Data Proposal", in *Just Security*, 31 August 2016, https://www.justsecurity.org/32619.

[30] To limit its scope, this report does not consider data gathering activities of intelligence agencies. Thus, unless otherwise specified, when referring to the process of "acquisition of e-evidence," this paper mainly refers to the investigation practices of law enforcement agencies.

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016 ISSN 2280-6164

access to data, especially when clearly in contradiction with privacy's traditions and current legal frameworks, should be avoided and, again, a more efficient mechanism of international cooperation should be devised.

ISSN 2280-6164

1. E-evidence and cross border data requests in France

by Vincent Joubert[31]

In July 2016, the French National Assembly and Senate voted to extend the state of emergency for six more months. First implemented on November 2015 following the terror attacks in Paris, emergency laws and powers have since been extended three times and are still in force today.[32] This exceptional legal state is of importance with regard to how French authorities seek digital evidence to investigate crime and terrorism related offences. Enforcing security in cyberspace requires an exhaustive set of legal, technical, organizational and human resources upon which governments rely to prevent and respond to acts of violence; however, considering the increasingly fast technological innovation cycles, which frequently introduce disruptive technologies in societies, enforcing security and law in the digital age also requires agile, adaptive, and cooperative frameworks.

Within the past ten years, French national authorities have developed appropriate capabilities to implement a comprehensive response to crime committed within or with the use of digital technologies. In order to fully comprehend how France has addressed the issue of collecting and using data for criminal investigations, we will first present the existing legal framework within the national jurisdiction; considering the recent circumstances France has had to face, the extraordinary powers granted by the implementation of the state of emergency must be outlined. Secondly, we will identify the international agreements France has developed to face the issue of collecting digital evidence outside its jurisdiction and finally, we will evaluate the possibility of European harmonization of relevant rules from French national authorities' perspective.

1.1 Legal framework for digital evidence gathering within national jurisdiction

The very first element to consider when examining the position of French national authorities regarding law enforcement in cyberspace is the existence – or non-existence, for that matter – of an official definition of what constitutes "digital evidence." From a legal perspective, an "evidence" covers a very wide set of elements – writings, oral testimonies, objects, recordings, etc., while the digital nature of such elements generally refers to information and communications

[31] Vincent Joubert is junior researcher at the Fondation pour la recherche stratégique (FRS).

[32] Alexandre Boudet, "La version 4 de l'état d'urgence est la plus musclée depuis novembre 2015", in *Huffington Post*, 27 July 2016, http://huff.to/2e1B8Uz.

ISSN 2280-6164

exchanged with the use of electronic devices. However, the development of digital technologies and associated use have considerably widened the nature of what can constitute digital evidence and how such evidence is collected, processed and used for criminal investigations.

1.1.1 Legal framework for the collection of digital evidence in the context of criminal investigations under ordinary circumstances

Considering that cyberspace is man-made, every technological innovation or new device connected to it will contribute to maintaining the ever-expanding and ever-evolving nature of the domain. In such conditions, the perimeter of the notion of "digital evidence" can therefore be very large and debatable. French national authorities have identified four aspects directly related to digital data and its use with respect to criminal investigations and law enforcement: the *Code des postes et des communications électroniques* identifies obligations relevant to internet service providers (ISPs) vis-à-vis individual users and public authorities; the *Code pénal* defines crimes and offences committed against or through the use of information and communication systems; while the *Code de procedure pénale* frames the legal requirements for digital evidence collection.[33] Under the laws, orders and regulations adopted and compiled in these codes, which together establish the basis of the legal framework for French national jurisdiction, however, what constitutes digital evidence is not directly defined.

Now of course, when talking about digital evidence, the notion of cybercrime immediately comes to mind. French national authorities have defined cybercrime in an official report ordered by the Ministries of Justice, Budget, Interior and Digital Economy in June 2013, as "the criminal offences attempted or perpetuated against or with the use of an information and communication system, primarily internet."[34] Two distinct legal situations come out of this definition: first, criminal activities perpetuated with the use of cyberspace. In this case, digital technologies serve as a capability used to commit criminal activities.[35] The other case refers to criminal activities perpetuated in cyberspace. Here, digital technologies are not simply the

[33] In addition, the Code de la sécurité intérieure specifies how intelligence services can gather information and data for security and antiterrorism purposes.

[34] See recommendation No. 1 in Groupe de Travail Interministériel sur la lutte contre la cybercriminalité, *Protéger les Internautes. Rapport sur la cybercriminalité*, February 2014, p. 12, http://www.ladocumentationfrancaise.fr/rapports-publics/144000372/.

[35] In its 2014 report, the Criminal Politics Evaluation Centre of the Ministry of the Interior has identified 475 criminal offences related to cybercrime – that is an offense committed with the use of or in cyberspace. A first category identifies 248 offenses for which the object or the device used to commit the offense falls into cybercrime perimeter. A second category identifies 181 offenses for which even though the crime does not fall into cybercrime perimeter, its realization required the use of an information and communication system and its utilization has been formally established. The third and last category lists 46 offenses identified in the Code des postes et des télécommunications which fall into the cybercrime perimeter. Application of the measures granted by the Code de procédure pénale, which we introduced here, covers all of those 475 criminal offenses.

ISSN 2280-6164

tools but also the target of the criminal activities. The underlying motivation or purpose may be financial, ideological, political or simply "for the fun of it," but any infringement that degrades, denies, destroys, disturbs or deceives information systems or networks and the data stored, exchanged and exploited on them is, according to the French law, punishable. That is precisely what the *Code pénal* defines in its articles 323-1 to 323-8.[36] Each article establishes the punishment for the different infringements we described – degradation, denial of access or use, destruction, disturbance, deception.

The *Code de procédure pénale*,[37] which represents the legal framework for investigation and prosecution of criminal offences, defines under what legal circumstances and specifies the legal procedures required to obtain digital evidence. First, article 94 establishes that information and communication systems and data are considered to be of legal standing for criminal investigations and prosecutions. Then, articles 100 to 100-7 establish the conditions in which national legal authorities can order interception of electronic communications for the purpose of criminal investigations. The content of "electronic communications" is further elaborated in articles 706-95 to 706-95-10, where it is established what elements the legal authorities are allowed to seize, under what circumstances and with respect to which procedures.

Interestingly, the *Code de procedure pénale* differentiates electronic communications from digital data; articles 706-102-1 to 706-102-9 indeed establish specific rules for the collection of digital data seized on information systems. It is specified that national legal authorities can order, for the purpose of criminal investigations,

> the implementation of a technical device that can allow, without the user's consent, to access digital data from anywhere, to record, store and transmit them to relevant authorities as they are stored in an information system, as they appear on a screen or device, as they are stored by the user or received by him through any audio-visual device (art. 706-102-1).

"Technical device" covers a variety of tools but most presumably refers to Trojan. The implementation operation can be executed by any qualified agent of the national authorities, that is, agents from national intelligence or defence services who have specific expertise and capabilities to carry out such operations. The demand must come from national legal authorities and be agreed by any of the other involved authorities – Prime Minister, Minister of Defence, Minister of Interior. Such operations can only be carried out for serious crimes as defined by articles 706-73 and 706-73-1 of the *Code de procedure pénale*; only in the most severe criminal cases national authorities can require the use of such invasive

[36] Code pénal, http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPENAL.rcv.

[37] Code de procédure pénale, http://www.legifrance.gouv.fr/WAspad/UnCode?code=CPROCPEL.rcv.

ISSN 2280-6164

tools like Trojans.

Moreover, articles 230-1 to 230-5 of the *Code de procedure pénale* establish that encrypted data can legally be decrypted for the purpose of criminal investigations, and specifies the associated procedures. For some categories of criminal offences,[38] qualified agents from national cybersecurity authorities can also be mandated to decrypt the data seized by national legal authorities.

Finally, in order to provide a full spectrum of capabilities to legal authorities in terms of digital evidence collection, articles 230-32 to 230-44 establish the conditions under which, and the procedures required to gain access to geographical localization of any object deemed relevant to criminal investigations; electronic devices are covered by the law, hence, the use of data to locate an object or an individual.

Article L34-1 of the *Code des postes et des communications électroniques* establishes the obligations by which national ISPs must produce specific information in the context of criminal investigations and prosecutions.[39] Article R10-13 of that same code then establishes what elements national ISPs must retain to facilitate criminal prosecution: identification information, data related to the type of equipment owned and used by the user, technical characteristics, date, time and length of the conversation, information related to any additional service used or accessed by the user, data allowing the identification of communications' addressees and finally the data allowing the identification of geographical location of the communications. The Code requires one year retention for such data.[40] The elements identified by this law allow the authorities to access most of the relevant data for criminal investigations. Telephone operators and national ISPs are obliged by law to give access to such elements if – and only if – legal authorities have issued the required requests. As for international ISPs, the Advisor to the Prefect in charge of the fight against cyberthreats at the Ministry of the Interior, Eric Freyssinet, confirmed that French justice set a precedent by allowing national authorities to send formal requests to obtain data and information to entities located outside France, hence validating the legal admissibility of formal demands to international

[38] Such as murder committed by an organized group; torture and acts of barbarity committed by an organized group; drug trafficking; kidnapping and false imprisonment committed by an organized group; human trafficking; felonies and aggravated misdemeanours relating to procuring; theft committed by an organized group; aggravated extortion; destruction, defacement or damage of a property committed by an organized group; counterfeiting money; terrorism acts; arms and explosives devices trafficking and usage; illegal migrants trafficking committed by an organized group; money laundering; organized crime; hijacking committed by an organized group: WMD trafficking; illegal mining activities committed by an organized group.

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

[40] Jones Day, *The Data Retention Saga Continues: European Court of Justice and EU Member states Scrutinize National Data Retention Laws*, August 2016, http://www.jonesday.com/the-data-retention-saga-continues-european-court-of-justice-and-eu-member-states-scrutinize-national-data-retention-laws-08-11-2016.

ISSN 2280-6164

ISPs.[41]

As we have established, French law covers the full spectrum of legal situations where the collection of digital evidence can be required. Whether it falls under the perimeter of cybercrime as defined by the French national legal authorities, or whether it is used for intelligence activities and special investigations, the legal framework defining the conditions, rules and procedures for digital evidence collection is exhaustive. Indeed, if we consider the whole picture, the protection level of data laid out by the legal framework is considered by most observers to be very high. France established a data protection law back in 1978, which grants every citizen with legal right to control and restrain data and information transferred to public or private organizations. The national legal framework for information and data collection and sharing we presented is subjected to the provisions established by the 1978 law. However, the law has been modified in January 2016 in order to expand and improve the legal protection of individuals' personal data. Indeed, the Minister for Digital Affairs Axelle Lemaire submitted a new law wherein the Commission Nationale de l'Informatique et des Libertés (CNIL), the national supervisory authority, is granted extensive roles, responsibilities and powers to control, advise and sanction public and private actors with regard to the applicability of the data protection legal framework.

Nonetheless, it is important to underline that those rules have been established for as part of the nation's regular legal regime. Unfortunately, as France – along with other European countries – faced repetitive terrorist attacks over the past two years, national authorities have decided to implement the "state of emergency" regime, which allows the implementation of exceptional legal and police measures. The examination of those measures is required to understand what new capabilities the state of emergency grants the authorities, and why it may be seen as problematic for some observers of civil society.

1.1.2 Legal and judicial powers under the state of emergency regime

When the French National Assembly and Senate voted the third extension of the state of emergency in July 2016, following the Nice attack and the assassination of a catholic priest a few weeks afterwards, not only did they vote for the extension of the extraordinary legal regime but they introduced a new "antiterrorism law." This text, amending an existing law, adds 19 new articles establishing measures of security and legal response to terrorism activities under the state of emergency regime, granting national authorities with more capabilities regarding special procedures such as "administrative search" – that is the legal right to search a suspect's house under simplified circumstances – or digital evidence collection (referred to as

[41] Interview with Mr Eric Freyssinet, Advisor to the Prefect in charge of the fight against cyberthreats at the French Ministry of the Interior, October 2016.

ISSN 2280-6164

"computer seizure").[42] The powers and capabilities granted to the intelligence services to conduct such operations have been remarkably strengthened and extended, prompting some observers to qualify it as "an unprecedented disruption of the balance between security and civil liberties."[43] Article 15 of this law establishes that intelligence services can now collect data of any person linked to an individual suspected of or convicted for terrorist activities, whereas the previous version of this law established that communications interception and data collection were only allowed towards an individual – and only one at a time – who's been identified as a potential threat to national security. National authorities have established that close family, friends, work relations or occasional relations who might be of interest for the purpose of the investigation can now be subjected to the same level of intelligence surveillance. Even though control measures are in place to make sure such investigations follow proper legal procedures, critics raised the issue of the human resources required to handle the increasing surveillance authorization demands – which seems to have been exaggerated, since the National Commission for the Control of Intelligence Techniques only issued a hundred authorizations since February 2016.[44] The national authorities justified this extension of surveillance measures by arguing that "the goal of these measures is to remove any doubt regarding the implication of family and relatives with specific technical sensors, hence allowing the intelligence services agents to focus on real national security threats."[45] Detractors called these intelligence techniques "mass surveillance" which questions "the very nature of the society we live in," but intelligence authorities counter-argue that "the level of control applied to French intelligence services is very high, so high that it actually surprises our foreigner partners, specifically when it comes to terrorist activities."[46]

In addition to this law, the French National Assembly and Senate have also voted for the implementation of "computer seizures" in the context of the state of emergency, which are deemed possible if an individual represents a possible threat to national security. Seizure of digital evidence for administrative investigations purposes is, under that law,[47] eased so that the police can seize digital devices and have access to electronic communications or encrypted data (art. 5). This new procedure is considered to be problematic by many observers, for several reasons; first, the new dispositions of this law are largely based on a previous version of the text which had been disapproved by the highest French legal authority, the Constitutional Council, whose role is to validate the conformity of laws with the French constitution. Dispositions of law elaborated for the previous version of the

[42] Law No. 2016-987 of 21 July 2016: *Loi prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste*, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032921910.

[43] Jacques Follorou, "La France s'engage dans la surveillance préventive de masse", in *Le Monde*, 28 July 2016.

[44] Jacques Follorou, "La France s'engage dans la surveillance préventive de masse", cit.

[45] Ibid.

[46] Ibid.

[47] Law No. 2016-987 of 21 July 2016, cit.

ISSN 2280-6164

text are included in the new law, and their constitutionality has since been validated because the new version includes safeguards to the protection of individuals' rights. In facts, the previous version of the text provided the authorities with the power to seize any electronic equipment or digital device during a criminal seizure without the consent of a judge. This disposition still exists but the new version of the law text now establishes that the equipment and devices seized during the search can only be exploited after legal authorities examine the circumstances of the procedure and validate the relevance of exploiting digital evidences. Second, following the extension of powers granted to the security authorities by the new law, search and seizure of electronic equipment and digital devices can affect the family and relatives of a suspected individual. It means that national authorities can seize any devices deemed necessary for the investigation. Third, according to the new dispositions of the law, legal authorities must validate the seizure within 48 hours and return the material within a fortnight. Even though national legal authorities validated the new law, many actors within the legal and judiciary community expressed their concerns, worrying that the law, voted a week after the attack in Nice, had been driven by an emotional reaction rather than by rationale.[48]

The multiple successive tragic events that hit France have led France's top political authorities to adopt and extend the extraordinary legal regime of the state of emergency. Under such a regime, judiciary and legal powers and procedures have been expanded, allowing national authorities to conduct more intrusive search and surveillance. Despite growing concerns and criticism from internal and external observers, the state of emergency is still applicable in France and with it the possibility for the intelligence services and legal authorities to collect and exploit more data as e-evidences. The relevance and usefulness of such extraordinary measures cannot be evaluated at this point, since the only elements of judgement would be ones provided by the authorities that first required these capabilities. Moreover, the very nature of intelligence counter-terrorism activities makes it complicated for external observers to provide an objective evaluation. Nevertheless, a national parliamentary investigation commission audited the effectiveness of the state of emergency and reported in early July 2016 that the extraordinary powers have not been identified as playing a key role nor as an improvement in the response against terrorist activities.[49]

French national authorities try to manage the delicate balance between privacy and the need to provide security to its citizens. Unfortunately, and especially at the moment, the very insecure international strategic environment provides temptation for more security and surveillance measures; however necessary, such

[48] Jean-Baptiste Jacquin, "Derrière la prolongation de l'état d'urgence, une nouvelle loi antiterrorist", in *Le Monde*, 22 July 2016; Syndicat de la Magistrature, *Prorogation de l'état d'urgence: notre courrier aux parlementaires*, 19 July 2016, http://www.syndicat-magistrature.org/Prorogation-de-l-etat-d-urgence.html.

[49] Sébastien Pietrasanta, "Rapport relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015", in *Documents d'information de l'Assemblée nationale*, No. 3922 (5 July 2016), p. 262, http://www.assemblee-nationale.fr/14/rap-enq/r3922-t2.asp.

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016
ISSN 2280-6164

measures should and, eventually, will remain extraordinary.

1.2 Legal framework for digital evidence gathering outside national jurisdictions

The French legal system is characterized by the superiority of conventions over laws, pending on the application of the convention by the other parties (as established by Article 55 of the French Constitution). Most of France's international cooperation with regard to mutual legal assistance (MLA) for criminal investigations is either based on the 1959 European Convention on Mutual Assistance in Criminal Matters, on the Schengen agreements application Convention, or on bilateral agreements. As a member of the EU, hence *de facto* member of Europol and Eurojust, France has signed and ratified many international treaties and conventions dealing with legal assistance between States.[50]

1.2.1 International mutual legal assistance agreements

National French law formally allows information and data transfer to international partners, as established by article L235-1 of the *Code de la sécurité intérieure*.[51] This article specifies that such information exchange must be part of international agreements signed by the national authorities and is to be executed by qualified authorities.

According to the data provided by the French Ministry of Foreign Affairs and Ministry of Justice, France has signed at least 61 bilateral conventions with international partners on mutual legal assistance in the case of criminal investigations and procedures.[52] Even though each convention is country specific, the terms of agreements include mutual cooperation when a criminal investigation arises; the basis of such cooperation lies on the mutual assurance of providing "the most exhaustive legal assistance in criminal matters" pending on the exceptions laid out

[50] As a member of Interpol, France actively participates to the information centralization and exchange processes that have been implemented by the agency to improve the cooperation amongst police forces – I-24/7, I-Link, e-extradition. Interpol's role in combating terrorism as a global platform for information exchange has been recognized by both the United Nations Security Council and the European Union. Their increased activities in the response to cybercrime and terrorism activities have played an important role in coordinating and identifying the elements legal and justice enforcement authorities required in the digital evidence domain.

[51] Code la sécurité intérieure, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000025503132.

[52] The countries are: Algeria, Argentina, Australia, Austria, Benin, Bosnia-Herzegovina, Brazil, Burkina-Faso, Cameroun, Canada, Central African Republic, Chad, China, Columbia, Congo, Croatia, Cuba, Djibouti, Dominican Republic, Egypt, Gabon, Germany, Hong Kong, Hungary, India, Israel, Italy, Ivory Coast, Jordan, Laos, Latvia, Macedonia, Madagascar, Mali, Mauritania, Mexico, Monaco, Mongolia, Morocco, the Netherlands, Niger, Paraguay, Peru, Romania, United Kingdom, Northern Ireland, Senegal, Serbia-Montenegro, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Thailand, Togo, Tunisia, UAE, Uruguay, USA, Vietnam.

ISSN 2280-6164

in the convention. Exceptions to the applicability of the convention are the core elements of each agreement and are established as part of the bilateral dialogue between France and the other party. Several new diplomatic bilateral initiatives have been taken by French national authorities with their respective counterparts in the area of digital information and data sharing for criminal investigations.

In January 2016, the French National Assembly voted two international conventions with the United States on mutual legal assistance in criminal matters. First signed back in 1998, the bilateral conventions have since been amended and expanded to include the consequences of the use of digital technologies in criminal offenses. The new conventions hence lay out the cooperation mechanisms in information and data exchange in the case of criminal matters – which include serious crimes and terrorist activities.[53] The information and data exchange was deemed necessary since there were no operational procedures in place between France and the United States – outside of Interpol's activities. The new conventions allow national authorities of both countries to have access to digital evidence in case of serious criminal investigations. Under the MLA agreements, France and the United States can require data and information as long as they are "adequate, relevant and not excessive in relation to the purposes of their transmission,"[54] that is to say the transmitted data only serves the purpose of the criminal investigation. The information is collected and stored only for the time of the criminal investigation and legal prosecution, must be listed and national authorities have the obligation to mention any mistake during the process. French authorities have demonstrated a high level of concern when dealing with privacy issues; the agreement with the United States was modified, at the request of French national authorities, to include specific guarantees for the application of a data protection level as established by the French law. The Government of the United States agreed to this request. As a result, France can refuse to transmit data if the request is deemed to threaten its national sovereignty, security, legal order or any other vital interest. Both parties must protect the collected data with appropriate measures and are subjected to control mechanisms carried out by an independent entity. If any personal data is illegally used, its owner is able to prosecute the faulty institution. Finally, this agreement is subject to the EU-USA data protection agreement, meaning that both France and the United States can suspend the application of the bilateral agreement if data protection conditions are not deemed respected by one party whether it is under the Privacy Shield or the French-American conventions.[55]

[53] French National Assembly, *Accord de coopération avec les États-Unis en matière d'enquêtes judiciaires*, 28 January 2016, http://www.assemblee-nationale.fr/14/cri/2015-2016/20160113.asp.
[54] Ibid.
[55] Ibid.

ISSN 2280-6164

1.2.2 Mutual legal assistance within the European Union

The first European instrument to regulate mutual legal assistance requests was the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters;[56] in 1978, a Protocol was added[57] and was followed by the 1990 Convention implementing the Schengen Agreement.[58] In 2000, member states signed a Convention on Mutual Assistance in Criminal Matters to supplement and facilitate the application of those conventions.[59] The 2000 Convention was reinforced in 2001 by a Protocol that focuses on mutual legal assistance concerning information on bank accounts or banking transactions.[60]

Under the 2000 Convention, member states can provide assistance with regard to criminal proceedings, administrative proceedings that may give rise to proceedings before a criminal court, proceedings relating to offences or infringements committed by a legal person. Cooperation is realized through exchanges of information between States' national judicial authorities; since 2001, member states have applied the principle of mutual recognition, which means that the judicial authorities of one member state will recognise decisions of another as being equivalent to its own. Following this principle and under the 2003 Council Framework Decision,[61] member states' judicial authorities can order the "freezing of property or evidence" for the purpose of a cross-border procedure to prevent the destruction, transformation, displacement, etc., of property. Evidence includes objects, documents or data which could be produced as evidence in criminal proceedings. France transposed the European Decision in national law; Title X of the *Code de procedure pénale* provides the dedicated legal framework for international mutual assistance.[62] Articles from Chapter I establish the general dispositions on mutual assistance in criminal investigations in terms of procedures, search warrant, digital evidence collection and transmission, as well as extradition. Chapter II

[56] Council of Europe, *The European Convention on Mutual Assistance in Criminal Matters*, Strasbourg, 20 April 1959, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/030.

[57] Council of Europe, *Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters*, Strasbourg, 17 March 1978, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/099.

[58] European Union, *The Schengen Acquis - Convention Implementing the Schengen Agreement*, Brussels, 19 June 1990, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:42000A0922(02).

[59] Council of the European Union, *Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 29 May 2000, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32000F0712(02).

[60] Council of the European Union, *Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 16 October 2001, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:42001A1121(01).

[61] Council of the European Union, *Council Framework Decision 2003/577/JHA of 22 July 2003 on the Execution in the European Union of Orders Freezing Property or Evidence*, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32003F0577.

[62] See Livre IV, Titre X (De l'entraide judiciaire internationale), Code de procédure pénale, cit.

ISSN 2280-6164

specifically transposes the European agreements on mutual legal assistance in criminal matters with dispositions on France's participation to the Eurojust agency, on the applicability of the 2003 European Council framework decision on confiscation and freezing of assets, the applicability of the 2006 European Council Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the member states,[63] and finally on the applicability of the European Council's 2009 Decision on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings.[64] Each of these Council Decision includes dispositions on information and data collection and exchange with respect to the application of the 2009 European data protection legal framework – pending the 2016 European Council Decision entry into force. In 2010, the French Senate also supported the implementation of the Directive proposal regarding the European Investigation Order in criminal matters submitted by several European member states; the French upper Chamber consensually considered the proposal relevant and useful to further improve mutual legal cooperation between European member states for evidence collection in criminal investigations.[65]

In the EU, the new Data Protection legal framework (2015) has been strongly supported by French national authorities – through the voice of the Minister for Digital Affairs Axelle Lemaire[66] – as well as by French euro-parliament members. The "Digital Republic" law text – which is being reviewed for final adoption – considerably expands the legal framework for digital content and the rights and obligations of users.[67] The abundance of texts at the national and European level – with the 2009 European Council Decision on privacy and electronic communications being reassessed – introduces the risk of confusion, though legal experts rather welcome the recent improvements in the legal arsenal. However, ambiguities have been pointed out by observers, specifically in the case of the Privacy Shield agreement between the EU and the United States; Minister of Justice Jean-Jacques Urvoas sent a letter to the European Union's Commissioner for Justice Vera Jourová underlining the need to improve safeguards on privacy

[63] Council of the European Union, *Council Framework Decision 2006/960/JHA of 18 December 2006 on Simplifying the Exchange of Information and Intelligence between Law Enforcement Authorities of the Member States of the European Union*, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32006F0960.

[64] Council of the European Union, *Council Framework Decision 2009/948/JHA of 30 November 2009 on Prevention and Settlement of Conflicts of Exercise of Jurisdiction in Criminal Proceedings*, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32009F0948.

[65] French Senate, *Initiative en vue d'une directive du Parlement européen et du Conseil concernant la décision d'instruction européenne en matière pénale*, 29 April 2010, https://www.senat.fr/ue/pac/E5288.html.

[66] French Ministry for the Economy, Industry and Digital Affairs, *Axelle Lemaire salue l'accord obtenu sur le règlement européen sur la protection des données personnelles*, 16 December 2015, http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/20235.pdf.

[67] Emmanuel Macron and Axelle Lemaire, "Projet de loi pour une République numérique", in *Documents d'information de l'Assemblée nationale*, No. 3318 (9 December 2015), http://www.assemblee-nationale.fr/14/projets/pl3318.asp.

ISSN 2280-6164

and prevent loopholes in the agreement.[68]

In a joint press conference in Paris on 23 August 2016 with German Minister of Interior Thomas de Maizière, France's Minister of Interior Bernard Cazeneuve called for the European Commission to change the law to give security agencies the ability to access encrypted data. He hoped such legislation would force firms to hand over crypto keys to police investigations in order "to equip our democracies with genuine tools to tackle the issue of encryption."[69] While acknowledging the importance of encryption for lawful activities such as protecting sensitive national information or financial transactions, Cazeneuve blamed certain communication applications that use end-to-end encryption saying they were problematic for security services and for criminal investigations. Calling on the European Commission to examine the possibility of enforcing the same rights and obligations on operators of any telecom or internet service offered to users in Europe, regardless of whether they are headquartered in Europe, Cazeneuve stressed out that such legislation would allow the investigation and magistrates services to identify, decrypt and access messages so they can be used as evidence. The new unified European legislation would allow member states' governments "to impose obligations on operators that prove uncooperative, particularly in order to remove illicit content or decrypt messages" in the context of criminal or terror attacks investigations.[70] French authorities therefore fully endorse[71] the EU Justice and Home Affairs Council conclusions on the fight against criminal activities adopted on 9 June 2016;[72] the Council proposed concrete measures and actions in three main areas such as streamlining MLA proceedings and, where applicable, mutual recognition related to cyberspace, improving cooperation with ISPs through the development of a common framework to request specific categories of data and launching a reflection process on possible connecting factors for enforcement jurisdiction in cyberspace. As the Council of the EU and its member states further investigate the actions required to improve legal cooperation, namely the possible grounds for enforcement jurisdiction that could be applied in cyberspace and a differentiated treatment of specific categories of data in criminal proceedings, it also enhanced the European Judicial Cybercrime Network supported by Eurojust. The position of French national authorities regarding the harmonization of the procedures to collect digital evidence at the European level is consistent with the

[68] Marc Rees, "Privacy Shield: les inquiétudes du garde des Sceaux adressées à la Commission européenne", in *NextINpact*, 8 June 2016, http://www.nextinpact.com/news/100148-privacy-shield-preoccupations-garde-sceaux-adressees-a-commission-europeenne.htm.

[69] French Ministry of Foreign Affairs, *Speech by M. Bernard Cazeneuve, Minister of the Interior, during the joint press conference with Mr Thomas de Maizière, German Minister of the Interior* (excerpts), Paris, 23 August 2016, http://basedoc.diplomatie.gouv.fr/vues/Kiosque/FranceDiplomatie/kiosque.php?fichier=baen2016-08-25.html#Chapitre2.

[70] Ibid.

[71] Interview with Mr Eric Freyssinet, Advisor to the Prefect in charge of the fight against cyberthreats at the French Ministry of the interior, October 2016.

[72] Council of the European Union, *Fight Against Criminal Activities in Cyberspace: Council Agrees on Practical Measures and Next Steps*, Luxembourg, 9 June 2016, http://europa.eu/!XX67Kg.

ISSN 2280-6164

conclusions of the Council: streamlining concrete actions and measures to unify legal frameworks is a priority to develop solutions enabling effective investigations in cyberspace.

ISSN 2280-6164

2. E-evidence and cross border data requests in Germany

by Anja Dahlmann[73]

In light of the recent terrorist attacks in Europe, the German Government approved several laws addressing national security concerns. A new law on data retention was issued in December 2015,[74] while the so-called Second Anti-Terrorism Package followed in August 2016.[75] Both legislations amended several laws, expanded the competences of the German law enforcement agencies (LEAs) and intelligence services, as well as enhanced inter-agency and international cooperation on these matters. The Anti-Terrorism Package was mostly a reaction to the 2016 terrorist attacks in Paris and Brussels. The fast-paced adoption of the package (less than six months) proves the then urgency of the matter for the German Parliament. An important point concerning digital evidence gathering is that LEAs acquired further competencies for international cooperation.

The first part of this section describes the existing legal options for the several German LEAs in order to obtain digital evidence. These include the interception of telecommunications, but also the surveillance of electronic communication on computers, to which service providers operating in Germany have to comply. However, limits to such criminal prosecution, especially concerning the right to privacy and the privacy of correspondence, posts and telecommunications, are envisaged in the German Constitution. The second part of the section addresses international cooperation with regard to criminal prosecution in the digital realm. Great emphasis will be placed on Germany's cooperation with the United States, as well as within the European Union. Ultimately, the analysis proves that, in recent years, the awareness towards the value of digital evidence in Germany has substantially increased, as several law extended the options for the gathering of digital evidence. In addition, the recent political statements illustrate the Government's willingness to contribute to the harmonization of this kind of criminal prosecution within the EU.

[73] Anja Dahlmann is research assistant at Stiftung Wissenschaft und Politik (SWP).

[74] Germany, *Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten* (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.

[75] Germany, *Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus* (Act to improve anti-terror information exchange in force), 26 July 2016, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s1818.pdf.

ISSN 2280-6164

2.1 Obtaining digital evidence within German jurisdiction

Digital evidence is collected accordingly to the police laws of the federal states, as well as national laws, such as the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz*, BKAG). Other relevant laws on digital evidence are: the German Criminal Code (*Strafgesetzbuch*, StGB), which establishes punishments for defined crimes, including several provisions on the so-called cyber-crimes. The German Code of Criminal Procedure (*Strafprozessordnung*, StPO) includes, among other things, rules on the use of technology for criminal prosecution. The Telecommunications Act (*Telekommunikationsgesetz*, TKG) regulates the telecommunications (including internet service providers) market and contains data protection and data retention terms. The Federal Data Protection Act represent complementary legislation to this framework.

2.1.1 Criminal prosecution

The German Criminal Code (StGB)[76] defines several cybercrimes, meaning criminal offences committed by means of electronic devices and/or via the internet. More precisely, the Code addresses data espionage (sec. 202a StGB[77]), the interception of data (sec. 202 StGB), acts preparatory to data espionage and phishing (sec. 202c StGB), reception of stolen data (sec. 202 StGB), computer fraud (sec. 263a StGB), forgery of data intended to provide proof (sec. 269 StGB), data tampering (sec. 303a StGB), computer sabotage (sec. 303b StGB), and the disruption of telecommunications facilities (sec. 317 StGB). Although the Criminal Code does not define the term data, section 202a StGB qualifies it to those pieces of information stored and processed by electronic, magnetic or other means.

German law enforcement agencies have several options in order to obtain digital evidence. For example, they can gain physical access to electronic devices and media that store the data or can cooperate with service providers, in case the data is stored on their servers. The latter option is limited to subscriber and traffic data, excluding content data, as it will be discussed in section 2.1.2. They may also wiretap telephones, search computer files through an online link or use a Trojan to monitor computer communications. Concerning the legal basis for implementing such measures, with regard to the physical access to storage devices, the general rules of procedure apply.

According to the German Code of Criminal Procedure (StPO),[78] the police is allowed to monitor and record the telecommunications of its citizens through wiretapping upon the authorization of a judge (sec. 100a StPO). In other words, this means that

[76] German Criminal Code, http://www.gesetze-im-internet.de/englisch_stgb.

[77] Most of the subsequent paragraphs refer to the limitation of data in sec. 202a, which restricts the term to data stored by electronic or magnetic means or means similar to that.

[78] German Code of Criminal Procedure, http://www.gesetze-im-internet.de/englisch_stpo.

ISSN 2280-6164

a service provider allows the entitled LEA to listen to a conversation similarly to what happens during a conference call. The provider then offers a digital copy of the conversation along with the traffic data (in such cases, physical access to the phone is unnecessary).[79] From a legal perspective, the implementation of wiretapping requires a suspicion of certain crimes, which include, high treason, counterfeiting of money, manslaughter, fraud and computer fraud, as well as tax evasion (sec. 100a(2) StPO). All law enforcement agencies are authorized to access and use the acquired data, as long as their collection does not violate private life.

In addition, based on their competencies, criminal polices offices and LEAs[80] (according to the legislation of each federal state) can use a special tool to monitor electronic communication: the Remote Communication Interception Software (RCIS), often referred to as "Staatstrojaner" or "Bundestrojaner" (*Quellen-Telekommunikationsüberwachung*, Quellen-TKÜ). The software takes the surveillance of communication one step further compared to section 100a of the StPO. By infiltrating the IT system, the software enables monitoring computer communication and other electronic devices before communications and data are encrypted.[81] The RCIS is legally limited to the interception of real-time

[79] See the website of the Federal Commissioner for Data Protection and Freedom of Information, "Überarbeitung des § 100a StPO (Telekommunikationsüberwachung)", in *Neuordnung der verdeckten Ermittlungsmaßnahmen im Strafverfahren*, http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/20061114_VortragEnders.html.

[80] The competence in terms of protection from security threats and criminal prosecution in Germany is streamed among several actors. According to article 30 GG, the police of the federal states is primarily responsible for the protection against threats. The police also supports the public prosecutor's office in matters of criminal prosecution. The police forces consist of several units, including the constabulary (*Schutzpolizei*) and the criminal investigation department (*Kriminalpolizei*). The latter is responsible for the prevention and prosecution of severe crimes, such as manslaughter, robbery, organized crimes, and the protection of the state. Police forces are, for instance, responsible for providing IT forensics services. At a national level, the Federal Police (*Bundespolizei*) is responsible for investigating crimes occurring on trains, national borders and in the airspace. In order to support the work of the police, each of the 16 federal state has a criminal police office (*Landeskriminalamt*). This is tasked with ensuring the protection from security threats, as well as conducting criminal prosecution for special criminal cases (e.g. corruption, drug trafficking, and cybercrime). Police forces also provide interregional support to local police within the federation. They also link to the police forces and the Federal Criminal Police Office (*Bundeskriminalamt*, BKA). The Federal Criminal Police Office is responsible for the protection against and prosecution of organized crime, dangers to constitutional organs and external affairs, crimes committedin foreign countries, domestic security, and internationally organized terrorism. Based on its mandate, the Federal Criminal Police Office is a key actor for the collection of digital evidence in Germany.

[81] The RCIS is considered a highly problematic tool to obtain digital evidence: amongst other things, it could be used to record audio files through the microphone and video files with the device's camera, thus constituting a clear violation of the personal and private residence, especially when the core area of private life is at stake. Furthermore, the spy software is reported to contradict basic forensic principles, as it is said to change the system it is supposed to "examine." Regardless of these allegations, the RCIS might not be as useful as the authorities hope it would be. For example, it seems that the software cannot be used to obtain data from programmes such as WhatsApp or Threema for technical and legal reasons. Firstly, in contrast to traditional telecommunication providers, they are not obliged to cooperate with LEAs; secondly, so far the RCIS could not be installed on mobile devices like smartphones or tablet computers because it only runs on Windows systems. See Florian Flade, "Spähsoftware Bundestrojaner ist kaum brauchbar",

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

communication (Skype), messaging software, as well as email conversations. Also, the RCIS must not scan unrelated programmes and documents, as this type of search would require a different legal basis (although the means used could be very similar). The Federal Constitutional Court decided that such an online search violates the integrity and confidentiality of information technology systems, which can only be justified based on a tangible danger for the State or human lives.[82] However, there is an ongoing dispute on the actual use of RCIS for purposes of criminal prosecution. In 2013, the Federal Public Prosecutor stated that it will not use the RCIS for criminal prosecution, unless the StPO explicitly allows it.[83] However, the RCIS could be used according to secs. 100a and 100b StPO.[84] In compliance with the BKAG,[85] the Federal Criminal Police Office's use of the RCIS is limited to protection against terrorist threats (para. 20i secs. 1, 2 BKAG).[86]

Based on a 2009 amendment to the BKAG, since February 2016 the Federal Criminal Police Office is officially allowed to use a version of the RCIS.[87] As the Chaos Computer Club (CCC) revealed in 2011, the Ministry of the Interior approved this programme after a previous version was found to exceed existing legal restrictions.[88] The Ministry of the Interior commissioned the Federal Criminal Police Office and the private company FinFisher to develop an upgraded version of the RCIS.[89] In order to protect the ongoing investigations, the Ministry of the Interior did not provide further technical information on the software.

As previously mentioned, in 2009 the BKAG was amended, by allowing the use of the RCIS, in order to combat terrorism more effectively.[90] However, in April

in *Welt*, 10 April 2016, http://www.welt.de/politik/deutschland/article154173376.

[82] Federal Constitutional Court, *Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07*, http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[83] Ulf Buermeyer, "Analyse: Gläserne Menschen per Bundestrojaner?", in *Heise online*, 24 February 2016, https://heise.de/-3116668.

[84] Federal Criminal Police Office, *Standardisierende Leistungsbeschreibung zur Quellen-Telekommunikationsüberwachung*, 29 February 2016, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.html.

[85] Germany, *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten* (Act on the Federal Criminal Police Office and the Cooperation between Federal and State Authorities in Criminal Police Matters), 7 July 1997, https://www.gesetze-im-internet.de/bkag_1997.

[86] The same scope applies to the online search by the Federal Criminal Police Office. See para. 4a, 20k BKAG. Ibid.

[87] Markus Beckedahl, "Neuer Staatstrojaner soll fast fertig sein (Update: Genehmigung wurde heute erteilt)", in *Netzpolitik*, 22 February 2016, https://netzpolitik.org/?p=113672.

[88] The assessment as well as a decision by the Federal Constitutional Court referred to the Bavarian Trojan known as "0zapftis", but several German LEAs used the same or a very similar software. See Chaos Computer Club, *Chaos Computer Club Analyzes New German Government Spyware*, 26 October 2011, http://www.ccc.de/en/updates/2011/analysiert-aktueller-staatstrojaner.

[89] Ulf Buermeyer, "Analyse: Gläserne Menschen per Bundestrojaner?", cit.

[90] Germany, *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt* (Act to counter the dangers of international terrorism through the Federal Criminal Police Office), 25 December 2008, https://www.gesetze-im-internet.de/bkaterrabwg/BJNR308300008.html.

ISSN 2280-6164

2016 the Federal Constitutional Court considered the amendment partially unconstitutional.[91] Although the law remains currently in force, it must be revised by 2018. One of the major points of criticism to the issue refers to the possibility of monitoring lawyers, doctors and journalists engaged in confidential conversations with their clients. However, clergymen, criminal defence lawyers and members of parliaments (sec. 53 para. 1 no. 1, 2, 4 StPO) do not fall under such provisions and cannot be under surveillance (para. 20c sec. 3 BKAG). The Court urged the Parliament to abolish the distinction between criminal defence lawyers and lawyers working in other legal branches. However, the Court had no reservations concerning the lack of protection for journalists and medical staff. Secondly, it decided to restrict data exchange between the Federal Criminal Police Office and foreign investigations agencies, including digital evidence. In particular, the Federal Criminal Police Office should ensure that the countries receiving digital evidence data respect human rights and data protection (although not necessarily matching German standards) and should also introduce some control and report mechanisms regarding data exchange with foreign agencies. Finally, the Federal Criminal Police Office is not allowed to use evidence (read: personal data) gathered for the purpose of counter terrorism in order to prosecute minor crimes.[92]

Regardless of how the data is obtained, German law does not limit the encryption of data. According to the rule that no man is bound to accuse himself (*nemo tenetur se ipsum accusare*), users cannot be forced to submit their passwords or decryption keys. Currently, companies are not compelled to enable LEAs to access their software through backdoors or to decrypt user's information. The Minister of the Interior, Thomas de Maizière stated that the German Government is not likely to change this measure and deems encryption as an important tool for safety and security purposes. Nevertheless, as de Maizière stressed, encryption must not become a security problem in itself.[93] Accordingly, the Minister intends to establish a new agency focused on the decryption of communications, the *Zentrale Stelle für Informationstechnik im Sicherheitsbereich* (Zitis). The agency will start operating with 60 IT-experts in 2017 and is supposed to expand to 400 employees by 2022. Zitis will support the Federal Police, the Federal Criminal Police Office and the Federal Office for the Protection of the Constitution.[94]

[91] Federal Constitutional Court, *Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09*, 20 April 2016, http://www.bverfg.de/e/rs20160420_1bvr096609en.html.

[92] Ibid.

[93] German Ministry of the Interior, *Zwei Jahre Digitale Agenda der Bundesregierung*, 7 September 2016, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2016/09/zwei-jahre-digitale-agenda.html.

[94] Georg Heil and Georg Mascolo, "Eine Behörde gegen das going dark", in *Tagesschau.de*, 23 June 2016, http://www.tagesschau.de/inland/behoerde-verschluesselung-101.html.

ISSN 2280-6164

2.1.2 Cooperation between service providers and national authorities according to the German TKG

The German Telecommunications Act (TKG)[95] requires national and foreign telecommunication service providers to support surveillance measures with content data and to provide subscriber and traffic data to LEAs upon request.

Section 110 TKG (complemented by further technical provisions in the Telecommunications Interception Ordinance, TKÜV[96]) regulates cooperation in case of surveillance measures mentioned in the previous section. According to this section, operators of telecommunications should develop their systems in accordance with LEAs surveillance measures. Section 112 TKG (in combination with sec. 163 StPO) requires telecommunication service providers to create a constantly updated database of all their costumers including their phone number, name, address, date of birth, address of the landline or device number of the mobile phone, as well as start of their contract (as listed in sec. 111 TKG). This applies to email too. The Federal Network Agency can access the databank and provide LEAs with requested data. These should be traceable, allowing the use of selectors. According to the annual report of the Federal Network Agency, in 2015 107 departments were entitled to request the data and 116 telecommunications service providers had to comply. In that year, about 220,000 requests based on a name and 7.4 million requests based on phone numbers were addressed to the Federal Network Agency. While the first number remains quite constant, the latter witnessed an increase of about 700,000 requests compared to 2014.[97]

In addition to this instrument, section 113 TKG in combination with section 100j StPO allows manual inquiry proceedings, meaning single requests in individual cases. Besides the data named in section 111 TKG, it enables LEAs to ask for data in order to create the contract between customer and service provider (secs. 3(3), 95 TKG, "customer data"), as well as IP addresses. LEAs are entitled to use this instrument for purposes of criminal prosecution and the protection against threats. In general, those inquiries must be in written form, but can provisionally be presented orally in case of imminent danger. The service providers must answer immediately and comprehensively and are not allowed to notify neither the concerned person nor third parties. Companies with more than 100,000 costumers must provide a secured electronic interface to be accessed by entitled LEAs.

[95] Telecommunications Act of 22 June 2004, http://www.bmwi.de/DE/Service/gesetze,did=21996.html.

[96] Telecommunications Interception Ordinance of 3 November 2005, http://www.bmwi.de/DE/Service/gesetze,did=24138.html.

[97] Federal Network Agency, *Jahresbericht 2015*, May 2016, p. 82-83, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2016/Jahresbericht2015.pdf?__blob=publicationFile&v=2.

ISSN 2280-6164

If companies do not show credible efforts to cooperate, the Federal Network Agency is authorized to demand a fine of up to 100,000 euros (sec. 115 TKG). However, if this provision is effectively enforced in cases involving foreign providers remains unclear. The TKG only covers telecommunication service providers but does not address over-the-top (OTT) messaging providers, which are crucial partners to obtain digital evidence nonetheless. Currently, the cooperation is voluntary and therefore problematic at times. A recent controversy involved German LEAs and Facebook. Apparently, in 2014, the company provided only one third of the requested data, claiming that the remaining two thirds were too vague or not sufficiently detailed to justify the disclosure of information.[98] In 2015, the number of answered inquiries rose to 42 percent, though.[99] As LEAs have extensively reported, direct cooperation is generally problematic because of the lengthy of the procedure to obtain the requested data due to delayed answers of the providers.[100] In early 2016, the Bundesrat urged the Federal Government to draft a bill regulating OTTs equal to ISPs.[101] So far, the Government has not drafted a respective law.

In case of severe crimes,[102] the German police forces, the Federal Criminal Police Office, and other agencies responsible for the protection against threats to public safety are allowed to request traffic (meta) data according to data retention terms (sec. 100g StPO, sec. 113b TKG).[103] This data contains information on the caller, the called person, the period, and the location of the call. This applies to text messages as well. With regard to telephone internet access, the user, IP address, and period of the internet access are of relevance (sec. 113b TKG).[104] Data regarding email – generic subscriber data, traffic data and content data – are not part of the retention.

[98] Since all users outside of the USA and Canada are costumers of Facebook Ireland Limited – not of US Facebook Inc. – the rules regarding Irish and European mutual legal assistance apply. The Council of Europe provides a good overview over the cooperation with foreign ISPs. See Cybercrime Convention Committee, *Criminal Justice Access to Data in the Cloud: Cooperation with "Foreign" Service Providers*, cit.

[99] Markus Reuter, "Doch nicht so kompliziert: So sieht das Formular aus, das Strafverfolger bei Facebook nutzen", in *Netzpolitik*, 9 August 2016, https://netzpolitik.org/?p=128641.

[100] See "Länder fordern Gesetz zur schnellen Datenherausgabe", in *Zeit Online*, 7 August 2016, http://www.zeit.de/digital/datenschutz/2016-08/facebook-nutzerdaten-herausgabe-strafverfolgung-gesetz.

[101] See Bundesrat, *Entschließung des Bundesrates zur Anpassung des Rechtsrahmens an das Zeitalter der Digitalisierung im Telekommunikationsbereich - Rechtssicherheit bei Messengerdiensten, standortbezogenen Diensten und anderen neuen Geschäftsmodellen* (Drucksache 88/16), 17 February 2016, http://www.bundesrat.de/SharedDocs/drucksachen/2016/0001-0100/88-16.html.

[102] According to sec. 100g StPO, those crimes are, for example, high treason, the formation of a terrorist organization, homicide or war crimes.

[103] In general, this excludes intelligence services, but the Bavarian Government defined the Bavarian Office for the Protection of the Constitution as a service responsible for the protection against threats to public safety, which contradicts the German distinction between prosecution services and intelligence services. See Lisa Schnell, "Bayerns Verfassungsschutz darf auf Vorratsdaten zugreifen", in *Süddeutsche Zeitung*, 7 July 2016, http://www.sueddeutsche.de/bayern/-1.3067677.

[104] The bill on data retention amended resp. introduced secs. 100g, 101a, 101b StPO and sec. 113a-113g TKG.

ISSN 2280-6164

All telecommunications service providers operating in Germany, although not OTT providers, must comply with the law on data retention. Following a formal judicial decision, the companies have to hand over the data to law enforcement agencies for prevention and prosecution purposes.

Most of the mentioned data have to be stored for ten weeks, while the location of the caller and the addressee must be stored for four weeks (sec. 113b TKG). The law does not define the term location, but regarding mobile phones, this means the radio cell and, possibly, the GPS coordinates. The distinction between location and other data can be problematic since the data on location is usually stored in a data set that subsumes all data. Therefore, different retention periods complicate the process substantially. In addition to that, companies are obliged to secure the data on the German servers that are monitored by the Federal Network Agency. Violations of the mentioned provisions can evoke claims for indemnity and compensation for immaterial damage. The current law on data retention was approved in October 2015. However, several members of the Parliament (specifically members of the Green Party) took legal actions against it through the Federal Constitutional Court.[105] The Court rejected a petition for a temporary order against the law in June 2016.[106] However, the complaint is still pending. Similarly, the internet provider SpaceNet and the IT association ECO also decided to bring the law to the administrative court in April 2016.[107] They criticized lack of compensation for the high costs of collection and storage, which will particularly affect small companies.[108]

2.1.3 Boundaries to criminal prosecution

The right to privacy and other fundamental rights limit any kind of criminal prosecution, especially surveillance measures. The right to privacy is a fundamental right defined by the Federal Constitutional Court as a crucial part of the right to self-fulfillment and general personal rights. It is based on article 2 para. 1 GG (self-fulfillment) in connection with article 1 para. 1 GG (human

[105] See Arne Meyer-Fünffinger, "Verdächtig ist jede und jeder", in *Tagesschau.de*, 3 September 2016, https://www.tagesschau.de/inland/vorratsdatenspeicherung-153.html.

[106] Federal Constitutional Court, *Beschluss der 3. Kammer des Ersten Senats - 1 BvQ 42/15*, 8 June 2016, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/06/qk20160608_1bvq004215.html.

[107] ECO, *eco Supports SpaceNet in Lawsuit against Blanket Data Retention*, 17 May 2016, https://international.eco.de/?p=5020.

[108] The estimation of costs varies from 260 million euros by the Federal Network Agency to 600 million euros by SpaceNet and ECO. See "SpaceNet und eco klagen gegen Vorratsdatenspeicherung", in *Süddeutsche Zeitung*, 9 May 2016, http://www.sueddeutsche.de/news/service/-dpa.urn-newsml-dpa-com-20090101-160509-99-877349. The estimation of the Federal Network Agency comprises only investments to update the systems and increase the storage facilities to meet the mandatory requirements; it does not number the costs for additional personnel. See Germany, *Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten* (Act introducing a storage obligation and a maximum retention period for traffic data), cit.

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016 ISSN 2280-6164

dignity).[109] Four fundamental rights complement the right to privacy: the privacy of correspondence, posts and telecommunications (art. 10 GG),[110] the privacy of the private residence (art. 13 GG), the right to the guarantee of the integrity and confidentiality of information technology systems, and the right to informational self-determination.

Concerning digital criminal prosecution and surveillance measures, article 10 GG constitutes the most relevant one. In particular the article establishes that: all measures to obtain digital evidence, e.g. the interception of telecommunication, as well as analysis of storage devices must not invade the core area of private life (German: *Kernbereich privater Lebensgestaltung*).[111] Consequently, if the gathering of digital evidence violates these fundamental rights, the findings cannot be used as evidence in trials regardless of the crime. Subsidiary to the above mentioned rights, the Federal Constitutional Court created the right to the guarantee of the integrity and confidentiality of information technology systems (art. 1 in combination with art. 2 para. 1 GG). The Court passed it to close the legal loophole left by article 10, since it only protects the process of communications but leaves the generated data on the electronic device unattended.[112]

As acknowledged by the Federal Constitutional Court in 1983, another derivate from the general personal rights is the right to informational self-determination. While the other guarantees are oriented towards criminal prosecution, the right to informational self-determination complements the above mentioned rights, focusing on data-protection. The Court ruled out that the control over personal data is the basis for self-fulfillment, freedom of speech and, therefore, is essential for a free and democratic society. This assumption is based on the idea that a lack of control could easily lead to self-censorship.[113]

While the Federal Data Protection Act (BDSG)[114] – and its regional counterparts, respectively – regulates most of the data processing procedures, several elements are not applicable to some operations conducted by the Federal Criminal Police Office and intelligence services. With regard to the Federal Criminal Police Office

[109] Basic Law for the Federal Republic of Germany (Grundgesetz, GG), https://www.gesetze-im-internet.de/englisch_gg.

[110] "Article 10 [Privacy of correspondence, posts and telecommunications]: (1) The privacy of correspondence, posts and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

[111] The actual definition of this concept is disputed among lawyers; the Federal Constitutional Court includes, for example, the sexuality of a person (Decision 75, 369 (380)) and a person's diary (Decision 80, 367 (374, 383)).

[112] See Federal Constitutional Court, *Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07*, cit.

[113] Federal Constitutional Court, *Urteil vom 15. Dezember 1983*, https://openjur.de/u/268440.html.

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

ISSN 2280-6164

these elements are, for instance, the restrictions to international exchange or the storage and use of data, as well as the duty to inform affected persons. The BKA operations include the support of the criminal investigation department of the police, international cooperation, the protection of constitutional organs and witnesses (secs. 2, 3, 5, 6 BKAG). The BDSG does fully apply to criminal investigation and the prevention of international terrorism (secs. 4, 4a BKAG).

2.2 International cooperation and the obtainment of digital evidence

Germany's international cooperation in criminal justice is based on the German Act on International Cooperation in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, IRG),[115] as well as on numerous bilateral and multilateral agreements. The IRG governs judicial cooperation between Germany and third countries in case no MLAT is in place. In these cases, it regulates the extradition, the enforcement of foreign sentences (and vice versa), as well as specific provisions regarding EU member states that, among other things, implement the European Arrest Warrant and other EU framework decisions. The IRG does not explicitly regulate the exchange of digital evidence for criminal prosecution but gives provisions on "tangible" evidence (secs. 66, 67 IRG). According to these articles, foreign LEAs can request the obtainment of evidence in case the criminal offence is prosecutable according to the German law ("dual criminality" requirement). The evidence can then be gathered if the law of the requesting state allows the seizure and no third party rights are violated. With regard to digital evidence, the latter requirement might be an obstacle for data held by German ISPs. These, indeed, would be third parties violated in their property rights.

Guidelines for courts, prosecutors and other LEAs complement the IRG (*Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten*, RiVASt).[116] Such guidelines include advice on 209 nations and nation-like entities. Section 77a of the guidelines offers advice on the surveillance of telecommunications according to section 100a StPO commissioned by foreign states in cases no MLATs or other agreements are in place. Accordingly, surveillance is admissible in case: the law of the requesting state allows the same investigative measure; the acquired information is only used to solve the crime specified in the request, and the conversation protocols are destroyed, as soon as they become unnecessary for the case. This guidance is accompanied by specific laws like the BKAG, which gives quite wide permissions regarding the transmission of evidence from surveillance

[115] Act on International Cooperation in Criminal Matters (AICCM), https://www.gesetze-im-internet.de/englisch_irg.

[116] Federal Ministry of Justice and Consumer Protection, *Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten* (Guidelines on Relations with Foreign Countries in Criminal Law Matters), 5 December 2012, http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_05122012_III19350B13002010.htm.

ISSN 2280-6164

measures to foreign agencies. In April 2016, the Federal Constitutional Court declared that the transmission itself is legal, but it should be amended by June 2018.[117] The receiving country must ensure that the protection of human rights and data meets German standards; also transferred data must only be used to solve the crime it was originally collected for. Finally, the court urged an appropriate control and report mechanism to supervise the transfer.

2.2.1 Cooperation with the United States

Criminal justice cooperation between Germany and the United States is based on three major accords: the agreement on combating the illegal trafficking of narcotics (1955/56), the agreement on mutual legal assistance and information exchange on criminal records (1961), and the treaty on mutual legal assistance.[118] In addition, the two governments organize an annual cyber-dialogue in which cybercrime is also discussed.[119]

The existing MLAT between Germany and the United States was signed in 2003 and amended in 2006.[120] The supplementary treaty incorporated provisions of the EU-US Mutual Legal Assistance Agreement of 2003. So far, no efforts towards an US-German agreement comparable to the agreement between the US and the UK regarding cross-border requests for data and evidence have been made.[121]

The search and seizure of (tangible) evidence is allowed under similar requirements as set by the IRG and RiVASt: the type of offence must be illegal in both countries, the request must include information justifying such action under the laws of the requested state, and the legislation of the requesting state must allow the seizure (Art. 11 para. 1 MLAT). The scope of use of the obtained evidence or information is quite broad compared to the RiVASt, especially after the amendment of article 15 para. 3 MLAT:

> The Requesting State may use any evidence or information obtained under this Treaty without prior consent of the Central Authority of the Requested State: 1. for the purpose of its criminal investigations and proceedings; 2. for preventing an immediate and serious threat to its public security, which, for the purposes of this Treaty, includes preventing the commission of

[117] Federal Constitutional Court, *Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09*, cit.

[118] Federal Ministry of Justice and Consumer Protection, *Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten*, cit.

[119] US Department of State, *Joint Statement on U.S.-Germany Cyber Bilateral Meeting*, Washington, 24 March 2016, http://www.state.gov/r/pa/prs/ps/2016/03/255082.htm.

[120] Treaty between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters, Washington, 18 April 2006, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl207s1618.pdf.

[121] David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests", in *Lawfare*, 16 July 2016, https://www.lawfareblog.com/node/11096.

ISSN 2280-6164

> serious criminal offenses; 3. in its non-criminal judicial or administrative proceedings directly related to a purpose set forth in subparagraph 1; 4. for any other purpose, if the information or evidence has been made public within the framework of proceedings for which they were transmitted, or in any of the situations described in subparagraphs 1, 2 and 3 of this paragraph.[122]

In practice, this section is somewhat restricted by the German Code of Criminal Procedure, especially the timely deletion of data and the predetermination for a specific purpose.

Interestingly, for the first time in a MLAT involving the USA, the treaty includes regulations on "special investigative techniques" (Art. 12), meaning surveillance of telecommunications and covert operations.[123] According to the treaty, requests for mutual legal assistance must come from and be addressed to the respective Ministries of Justice as central authorities or the competent authorities named in the appendix to the Treaty.[124] In addition, German police forces can contact Interpol or the FBI within the limits of their competencies in order to gather police documents and information, to investigate the location of a person or to question suspects and witnesses.[125]

Concerning the gathering of evidence in cyberspace, cooperation between German LEAs and American ISPs mostly occurs on a voluntary basis, as permitted under the US Electronic Communications Privacy Act (ECPA).[126] This procedure avoids an official MLAT request, but the German LEAs depend on the goodwill of the providers. Consequently, the process can take a long time, the transmitted data might be incomplete or the provider might not reply at all. Thus, several German politicians urged for enhancing collaboration with foreign service providers but, instead of aiming at negotiating a new treaty, they are calling for a new national law.[127]

[122] Treaty between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters, cit.

[123] See Letter of Submittal dated 14 June 2004 in US Senate, Mutual Legal Assistance Treaty with Germany. Message from the President of the United States, p. V-VI, https://www.congress.gov/treaty-document/108th-congress/27/document-text.

[124] Treaty between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters, cit., p. 1632-1633.

[125] Federal Ministry of Justice and Consumer Protection, *Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten*, cit.

[126] Cybercrime Convention Committee, *Criminal Justice Access to Data in the Cloud: Cooperation with "Foreign" Service Providers*, cit.

[127] See "Länder fordern Gesetz zur schnellen Datenherausgabe", cit.

ISSN 2280-6164

2.2.2 Cooperation and harmonization within the EU and the Council of Europe regarding rules to obtain digital evidence

Within the framework of the European Union and, specifically of the Council of Europe, Germany adopted several agreements and conventions on judicial cooperation: the European Convention on Mutual Assistance in Criminal Matters and its protocols (Council of Europe), the Schengen Agreement, the Convention on Cybercrime ("Budapest Convention"), the Prüm Convention (multilateral, partially transposed to EU law), the European Convention on Mutual Assistance in Criminal Matters and its protocol, as well as the European Investigation Order (Directive of the European Parliament and the EU Council).

In 2001, Germany signed the Convention on Cybercrime, which entered into force in July 2009. Aside from few minor reservations,[128] Germany managed to adopt the Convention. For example, the cybercrimes mentioned in the first section were added to the German Criminal Code.[129] Furthermore, many of the existing, general provisions were sufficient, rendering specific new regulation unnecessary.[130]

The European Investigation Order of 2014 will have to be transposed into German law by 22 May 2017. The Government drafted a corresponding amendment of the IRG in July 2016. This is supposed to transfer the Order as directly as possible into German law.[131] According to the Ministry of Justice, the amended law would enhance transparency, accelerate the procedures, and harmonize the necessary forms. Therefore, the European Investigation Order would lead to a further integration, replacing traditional instruments of mutual legal assistance.[132]

[128] Reservation contained in a Note verbale from the Permanent Representation of Germany deposited with the instrument of ratification, on 9 March 2009: "The Federal Republic of Germany declares that it avails itself of Article 42 of the Convention to the extent that (a) Article 6, paragraph 1.a.i, as relates to "devices", and sub-paragraph b shall not be applied, (b) the attempt to commit the acts specified under Article 3 shall not be established as criminal offence under national law, and (c) requests for expedited preservation of stored data under Article 29 may be refused on the ground that dual criminality is not given, provided there is reason to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled, unless the offence in question is an offence established pursuant to Articles 2 to 11." See the Budapest Convention's website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations.

[129] Sections 202a-202c StGB. See Germany, *Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität* (41st Criminal Law Amendment Act to Combat Computer Crime), 7 August 2007, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl107s1786.pdf.

[130] Cybercrime Convention Committee, *Assessing Implementation of Article 13 Budapest Convention on Sanctions and Measures*, Strasbourg, Council of Europe, 25 July 2016, p. 393-412, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ab6ab.

[131] See Federal Government, *Entwurf eines Gesetzes zur Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen*, 20 July 2016, http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/InternationaleRechtshilfeStrafsachen.html.

[132] Federal Ministry of Justice and Consumer Protection, *Kabinettsbeschluss für eine effektivere Rechtshilfe*, 20 July 2016, http://www.bmjv.de/SharedDocs/Artikel/DE/2016/07202016_EU_Ermittlungsanordnung.html.

ISSN 2280-6164

However, the German Federation of Judges (*Deutscher Richterbund*) criticized the Order arguing that it misses the chance of establishing a comprehensive regulation able to simplify cross-border cooperation.[133]

The latest development of the German involvement in EU criminal matters is a joint Franco-German statement on the enhancement of domestic security in the European context. Overall, two aspects deserve special attention. First, although both Ministers of the Interior stated the importance of encryption in several occasions, they criticize it for being an obstacle in the fight against terrorism. Therefore, they plan to exchange best practices and ideas on how to deal with encrypted communications. Second, they want to hold ISPs accountable in every country they offer their services – independently from the location of their headquarters. De Maizière, the German Minister of Interior, emphasized the importance of further European harmonization to strengthen national LEAs as well as the European Union.[134] The far-reaching requests of this initiative illustrate once more the current shifts in the perception of threat and, similarly, towards the extensive adoption of security measures.

In light of this development, Germany's support for further harmonization at the EU level does not seem unlikely. Nevertheless, the relatively high level of data protection or constitutional boundaries might ultimately limit these approaches.

[133] German Federation of Judges, *Stellungnahme zum Referentenentwurf zur Umsetzung der Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen*, Berlin, April 2016, http://www.drb.de/fileadmin/docs/Stellungnahmen/2016/DRB_160413_Stn_Nr_07_Umsetzung_EEA_Richtlinie.pdf.

[134] German Ministry of the Interior, *Europe Generates Added Value in Security-Related Matters*, 23 August 2016, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/EN/2016/08/joint-statement-de-maiziere-cazeneuve.html.

ISSN 2280-6164

3. E-evidence and cross border data requests in Italy

by Tommaso De Zan[135]

In March 2015, during a parliamentary debate on new measures to counteract terrorism, a new provision proposed by the Government sought to modify article 266bis of the Italian Code of Criminal Procedure.[136] By allowing "the employment of tools or software to consent the remote acquisition of communications and data stored in information systems," the new law aimed to restrict terrorists and criminals' room for manoeuvre in cyberspace and to provide Italian police with a strong investigative tool to prevent the kind of violent terrorist attacks that had shattered France.[137] Despite not being approved, the new provision unleashed strong statements of rebuttal by privacy activists, who argued that such an instrument would have granted unprecedented surveillance powers to the Government. Actors participating in the debate, however, limited themselves to curbing the use of surreptitious malwares by law enforcement agencies rather than taking a broader and more balanced perspective on the role of digital evidence in criminal investigations.

Going beyond this debate, and trying to mitigate the surveillance fears it elicited, this section describes the issues at stake when authorities prosecute crime in cyberspace, and underlines the evident importance of digital data evidence in Italian criminal investigations. Firstly, the section summaries the main regulations that shape how digital evidence is collected, and further presents a brief analysis on the major factors determining the process of collection. Secondly, it sheds light on judicial cooperation between Italy and the USA, and between Italy and other EU member states. Finally, it provides an overview of a new legislative provision of the Code of Criminal Procedure that, on paper, Italian authorities could evoke to obtain data stored abroad: article 234bis.

135 Tommaso De Zan is junior researcher at the Istituto Affari Internazionali (IAI). The author wishes to thank Alberto Cisterna, Antonio Gammarota, Stefano Quintarelli, Federica Resta and the numerous officials that have provided their feedbacks to the present section. The author particularly wishes to thank Stefano Aterno, Giovanni Nazzaro and Giuseppe Vaciago for their invaluable inputs.

136 See debate in the Justice Committee, 18 March 2015. Chamber of Deputies, Government bill: *Conversione in legge del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo...*, http://www.camera.it/leg17/126?tab=4&leg=17&idDocumento=2893.

137 "Decreto anti-terrorismo, così la polizia potrà accedere ai dati dei pc degli italiani", in *La Stampa*, 25 March 2015, http://www.lastampa.it/2015/03/25/italia/politica/decreto-antiterrorismo-cos-la-polizia-potr-accedere-ai-dati-dei-pc-degli-italiani-r8q16JkWdhDSVnavwVyMnK/pagina.html.

ISSN 2280-6164

3.1 The collection of digital evidence within Italian jurisdiction

This section outlines the national legislative framework in which the collection of digital evidence by Italian authorities takes place. As in the previous case studies, it takes a close look at a number of key regulations regarding data retention and the so-called "compulsory services," those services that providers need to perform in cooperation with judicial and law enforcement authorities. The section also delves into the principal articles of the Italian Code of Criminal Procedure (*Codice di procedura penale*, CPP),[138] which mainly regulates the collection of digital evidence and its use in criminal proceedings. It finally examines the latest developments of a highly sensitive issue in Italy: the use of the Trojan in the context of interceptions.

3.1.1 Data retention and "compulsory services"

Data retention refers to the period of time internet or telecommunications service providers can store data for regulatory or compliance purposes: it is "all about what, where and how long data should be stored or archived."[139] Data retention is essential for criminal investigations, as the time period during which providers store data determine the availability or lack thereof of digital evidence that can be used to prosecute a crime. In Italy, data retention terms are outlined in article 132 of the Privacy Code.[140] The article stipulates that, "with a view to detecting and suppressing criminal offences," providers shall retain telephone traffic data for 24 months, electronic communications traffic for 12 months, and unanswered calls for 30 days. It also declares that the Ministry of the Interior and the judicial police may order IT and/or internet service providers and operators to retain data, (although not content), according the arrangements specified above and for no longer than 90 days, also in relation to requests made by foreign authorities, in order to carry out pre-trial investigations for the detection and suppression of specific crimes. Data retention terms may be extended, on grounds to be justified, up to six months.

Nonetheless, data retention terms as presented above were supplanted by the approval of Law No. 21 of 25 February 2016 ("*Decreto Mille Proroghe*"), which forces providers to retain telephone and electronic communications traffic data, excluding content, until 30 June 2017, to detect and suppress serious crimes, including terrorism.[141] These retention terms will no longer be in place starting from July 2017, unless a new regulation prolongs them.[142] This decision was reproached by

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

[139] Techopedia online, IT Dictionary, https://www.techopedia.com/definition/31812.

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

[141] To see the changes to article 132 brought by the "Decreto Mille Proroghe", see ibid., p. 89, footnote 39.

[142] Jones Day, *The Data Retention Saga Continues*, cit.

ISSN 2280-6164

the Italian Data Protection authority and other experts, suggesting that, following the repeal of the Data Retention Directive by the European Court of Justice, which found the EU had exceeded the limits of proportionality in its data retention terms,[143] the Italian Government and the Parliament should have intervened to limit data retention and/or its use and access by national authorities.[144]

In addition to the Privacy Code, the Electronic Communications Code (*Codice delle comunicazioni elettroniche*)[145] contains an important provision that is important to mention in the context of investigations, even though it does not specifically relate to the collection of digital evidence. In the Code, article 96 elucidates the so-called "compulsory services" (*prestazioni obbligatorie*) that all "operators" (including non-EU) that are authorized, pursuant article 25, to offer their services in Italy, including internet service providers, must afford to Italian judicial authorities. It is important to underline here that service providers such as Google, Facebook, Skype (etc.), in other words those providing over-the-top (OTT)[146] or information society[147] services are excluded from delivering these compulsory services. OTT service providers are not compelled to deliver these compulsory services as they do not have to receive an authorization pursuant article 25 to operate in Italy.[148] Specifically, article 96 states that operators are compelled to provide, upon requests by competent judicial authorities, services such as interception of communications and delivery of information (data). Although a decree fully specifying these compulsory services has not been issued by the Justice and Economic Ministries yet, there exists an unofficial list detailing them.[149]

[143] Court of Justice of the European Union, Judgement of the Court in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8 April 2014, http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

[144] Guido Scorza, "Conservazione dei dati di traffico telefonico e telematico: una proroga lunga dieci anni", in *Avvocato del diavolo*, 13 February 2016, http://scorza.blogautore.espresso.repubblica.it/2016/02/13/conservazione-dei-dati-di-traffico-telefonico-e-telematico-una-proroga-lunga-dieci-anni.

[145] 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.

[146] Ilsa Godlovitch et al., *Over-the-Top (OTTs) Players: Market Dynamics and Policy Challenges*, Brussels, European Parliament, December 2015, http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)569979.

[147] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031.

[148] Interview, Rome, October 2016.

[149] According to Giovanni Nazzaro, these compulsory services are: (1) Users' personal data information (data given by the user at the time of the activation of the service); (2) Interception of communication (content and metadata); (3) Metadata; (4) Account's localization (mobile phone communication); (5) Account's identification; (6) Interruption of services (such as email services); (7) Traffic data's history; (8) Seizure of content. See: Giovanni Nazzaro, "Le prestazioni obbligatorie per l'autorità giudiziaria come disciplina studio", in *Sicurezza e Giustizia*, Vol. 4, No. 2 (2014), p. 18-19, http://www.sicurezzaegiustizia.com/?p=9395.

ISSN 2280-6164

3.1.2 E-evidence in the Italian Code of Criminal Procedure

Although the provisions outlined above have an important role in shaping how criminal investigations are conducted, the collection of digital evidence in Italy is mainly regulated by the Code of Criminal Procedure (CPP), in particular articles 244, 247, 248, 254bis, 259, 352, 354, 359, 360.[150]

Article 244 (Cases and methods of inspections) regulates "digital inspection." It establishes that the inspection of persons, places and objects occurs only if authorized and with the aim to ascertain the evidence of a crime. The judicial authority may order that an inspection should be performed by means of descriptive and photographic tools and any other technical operations, also by means of information systems, by adopting the technical measures aimed at guaranteeing the preservation of the original data and avoiding their alteration.

The object of article 247 (Cases and methods of searches) focuses on "digital search." It declares that if there are reasonable grounds to believe that data, information or software of the prosecuted crime are to be found within an information system, although protected by security measures, a search is ordered, by adopting the technical measures aimed at guaranteeing the preservation of the original data and at avoiding their alteration.

Article 248 (Request for delivery) maintains, if a specific object is sought through search, that the judicial authority may ask its delivery. If the object is handed in, the search will not be activated. To identify what should be seized, the judicial authority or the judicial police can examine databases, documents and correspondence, including data, information and software. In case what has been searched is not handed over, the judicial authority shall perform a search.

Article 254bis (Seizure of electonic data at the premises of providers of computer, electronic and telecommunication services) posits that the judicial authority, when it orders the seizure of data from internet services or telecommunications providers, including traffic and location data, might decide to acquire the sought data by copying them on a suitable medium, ensuring that the collected data are identical to the original ones and that they cannot be modified.

Article 259 (Custody of seized objects) suggests that those who have the custody of data need to ensure that the data will not be altered or accessed by third-parties, unless specified by the judicial authority.

[150] Stefano Aterno, *Digital Forensics*, 2014 (unpublished). Other articles relating to the issue, which are however out of the scope of the present section, are articles 226 and 252. The rest of the articles that have a profound impact on criminal investigations, namely articles 189, 234bis, 266bis, will be discussed in the next sections. English translation provided by Gialuz Mitja, Luparia Luca and Scarpa Federica (eds.), *The Italian Code of Criminal Procedure. Critical Essays and English Translation*, CEDAM and Wolters Kluwer Italia, 2014.

ISSN 2280-6164

Article 260 (Sealing of seized objects. Perishable objects. Destruction of seized objects) concludes that the judicial authority shall order a copy of the documents and the taking of photographs or other reproductions of the seized objects which could be altered or are difficult to keep in custody [...]. Data, information or software should be copied on suitable media devices, through a procedure that ensures the originality of the copy and which avoids its alteration [...].

Article 352 (Searches) maintains that, in the event of flagrante delicto, the judicial police can search information systems, even those protected by security measures, through technical procedures that are aimed at preserving the originality and integrity of data, when they have reasonable grounds to believe that, in these information systems, one could find data, information, software or evidences relevant to the crime which may be erased or modified.

Article 354 (Urgent checks of the scene, objects and persons. Seizure) specifies that if there is danger that evidence ("objects, traces, or locations") may be dispersed or will be altered, and the judicial authority has not assumed the control of the investigation, the judicial police shall conduct the needed ascertainments and checks on the conditions of the scene and objects thereof. In relation to data, information and software or information systems, the judicial police shall adopt all necessary measures to ensure the preservation and integrity of data, and to avoid third-party access. When possible, they shall immediately produce a copy of the data on an adequate medium, following a procedure that ensures originality and integrity. If necessary, criminal police will seize the evidence and objects pertaining to it.

Article 359 (Technical consultants of the Public Prosecutor) compels "consultants" to provide their technical services when nominated by the judicial authority, when the judicial authority asks to perform any technical operation requiring specific competencies.

Article 360 (Non-repeatable technical ascertainments) sustains that, if ascertainments foreseen by article 359 regards persons, objects or locations which are subject to change, the judicial authority warns the investigated person, the victim and their lawyers about the appointment of a technical consultant, for the assignments of non-replicable technical ascertainments. Lawyers have the right to participate in the ascertainment and to formulate observations and reservations. If, prior to the assignment, the investigated person requests a special evidentiary hearing, the judicial authority shall cancel the ascertainment. Notwithstanding that, such ascertainments shall be done if a delay may compromise their results. Finally, if the judicial authority decides to go ahead with an ascertainment, notwithstanding lack of urgency and explicit reservations by the investigated person, results deriving from the ascertainment cannot be used in trial.

ISSN 2280-6164

3.1.3 The Trojan horse and the issue of interceptions

Although controversial and subject to acerbic debate, the collection of digital evidence in Italy may also occur through the installment of the Trojan horse ("*captatore informatico*" or "*agente intrusore*," but also "*troiano*") in the suspect's device by law enforcement agencies or third-parties acting upon request. Despite numerous judicial cases having revealed its use, the topic continues to be highly sensitive because of the absence of specific laws regulating its deployment. Discussions upon the issue have become even more heated as the use of the Trojan has been associated with the topic of interception, a strongly divisive theme in Italy. Outcries by privacy activists deploring the use of the malware, recent controversial legislative initiatives and new verdicts of the Supreme Court of Cassation, the highest court of appeal in Italy, have all elicited a fierce debate that the ongoing reform of criminal procedures ("*riforma del processo penale*") has taken aim to address. So far, the use of the Trojan for criminal investigation purposes has found legislative cover in articles 189, 266 and 266bis of the CPP.[151] In a few words, article 266bis (Interception of computer communications or telecommunications) allows the interception of communications occurring between information systems in order to investigate serious crimes. On the other hand, article 189 (Evidence not covered by rule) states that, when a type of evidence is not regulated by law, as in the case of the evidence collected by the Trojan, the judge might use it in a trial only if suitable to establish the facts and if it does not compromise the moral freedom of a person. However, advancements in the sophistication of malwares – the possibility of recording conversations and "intimate moments" through the activation of the microphone and the video-camera of the infected device,[152] and the possibility of obtaining content data stored in the device and those flowing in and out – have fortified the need to legislate upon the Trojan's use.

A legislative initiative to regulate the use of the Trojan in criminal investigations was made even more urgent following two contrasting verdicts recently issued by the Supreme Court of Cassation.

In May 2015, the Court characterized as "invasive and unlawful," the acquisition of a device's content through the Trojan.[153] Also referring to article 8 of the European Convention on Human Rights, the Court argued that the activation of the video-camera and the microphone of the targeted device had exceeded national legislation, as the software performed an interception that was not restricted in time or location. To execute such an "invasive interception," nonetheless, law

[151] Pasquale Angelosanto, "Le intercettazioni telematiche e le criticità del data retention nel contrasto alla criminalità organizzata", in *Sicurezza e Giustizia*, Vol. 4, No. 4 (2014), p. 8-13, http://www.sicurezzaegiustizia.com/?p=10750.

[152] This type of recording would generate an "environment interception" (*intercettazioni ambientali*).

[153] Supreme Court of Cassation, *Sentenza n. 27100 ud. 26/05/2015*, 26 May 2015, http://www.penale.it/page.asp?IDPag=1201.

ISSN 2280-6164

enforcement should have sought prior approval by the judicial authority, specifying when and where the interception was to take place.[154]

In April 2016, the Court seemed to partially revise its judgment with verdict No. 26889,[155] introducing some instances in which the deployment of a Trojan could be allowed. The court declared it is possible to perform an interception with a Trojan to investigate serious felonies, such as those connected to organized crime and terrorism, "within private residences," without prior consent by the judicial authority, and even if there is no certainty that the crime is being committed at the time of the interception.[156] The verdict was met with skepticism by many. Whereas according to some the sentence was "myopic," as it was not fully and holistically evaluating the use of Trojan in criminal proceedings,[157] others urged the Parliament to take action to avoid leaving judges with the power to decide about the level of interference within citizens' privacy.[158]

It is against this backdrop that numerous legislative attempts have taken aim at regulating the use of the Trojan horse. Nonetheless, all of them have failed so far.

In early 2015, during discussions at the Chamber of Deputies concerning a new anti-terrorism law, an amendment initially modified article 266bis of the CPP, allowing the interception of communication between information systems "also through the employment of tools or software to consent the remote acquisition of communications and data stored in information systems."[159] The new provision, severely rebuked by the President of the Italian Data Protection Authority (DPA) Antonello Soro, was later scrapped by the Government in the final version of the law, which was approved on 31 March 2015.[160] Similarly, in December 2015, PD

[154] The Court had two main reasons to motivate its decisions: (1) taking into account article 15 of the Italian Constitution, the "environment interception" should occur in a well-circumscribed and previously identified location, and not everywhere; (2) the second issue concerned the activation of the video camera of the targeted device and thus the possibility of video-recording inside a private residence. The recording activity – if executed by the judiciary police – is to be considered "atypical evidence" and thus should be admitted by the judicial authority. To put it simply, in the case considered, the mere possibility of "using" the collected evidence, rather than the process of acquisition, was questioned.

[155] Supreme Court of Cassation, *Sentenza n. 26889 ud. 28/04/2016*, 1 July 2016, http://www.cortedicassazione.it/corte-di-cassazione/it/det_penale_sezioni_unite.page?contentId=SZP18700.

[156] Federico Nejrotti, "La Cassazione dice sì al trojan di Stato per la criminalità organizzata", in *Motherboard*, 4 July 2016, http://motherboard.vice.com/it/read/cassazione-trojan-di-stato-criminalita-organizzata.

[157] Monica Senor, "Se i captatori informatici diventano la cartina di tornasole delle nostre libertà fondamentali", in *Filodiritto*, 13 July 2016, http://www.filodiritto.com/articoli/2016/07/se-i-captatori-informatici-diventano-la-cartina-di-tornasole-delle-nostre-libert-fondamentali.html.

[158] Fabrizio Assandri and Paola Italiano, "Intercettazioni hi tech, appello dei docenti: 'Tutelare la privacy'", in *La Stampa*, 28 July 2016, http://www.lastampa.it/2016/07/28/cronaca/intercettazioni-hi-tech-appello-dei-docenti-tutelare-la-privacy-EpksjGC7W7lYCxIczuR9IO/pagina.html.

[159] Chamber of Deputies, Government bill: *Conversione in legge del decreto-legge 18 febbraio 2015, n. 7, recante misure urgenti per il contrasto del terrorismo...*, cit.; "Decreto anti-terrorismo, così la polizia potrà accedere ai dati dei pc degli italiani", cit.

[160] Garante per la protezione dei dati personali, *Soro: seria preoccupazione per emendamenti*

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

congresswoman Maria Gaetana Greco sought to modify article 266bis by allowing the use of the Trojan for criminal investigations.[161] This attempt was again reproached by many, who suggested that "this bill would allow the employment of the Trojan in thwarting online defamation, which is madness." In saying so, commentators suggested that the use of such a privacy invasive instrument should be consented only to investigate serious crimes.[162] However, this law proposal still has to be discussed.

The current draft law on the reform of the CPP (*Riforma del codice di procedura penale*) is the latest attempt in Italy to regulate the use of the Trojan. The Senate Justice Committee approved the reform in August 2016 and the new law is now under discussion on the Floor of the Senate.[163] The text under discussion tried to regulate the deployment of the Trojan as an "environment interception."[164] According to the new reform, the activation of the microphone or video-camera occurs when the judiciary police or authorized personnel requests it, and not from the start, when the Trojan is downloaded by the intercepted person. The personnel deploying the malware must report when the recording starts and ends. The Trojan must be used for investigating serious crimes (art. 51 para. 3bis and 3quater CPP) and can start recording in the victim's private residence, but only if the crime is being committed at the time of the registration. Furthermore, the content of the interception should be solely transferred to the competent judicial authority's office in order to guarantee the integrity and originality of the data intercepted; the malware should be uninstalled at the end of the registration. Finally, the technical features of the Trojan should comply with the specifications issued by a ministerial decree.[165]

approvati a DL antiterrorismo, 24 March 2015, http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3807700; *DL antiterrorismo: Soro, apprezzamento per le modifiche apportate al testo*, 26 March 2015, http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3813728.

[161] Chamber of Deputies, Law proposal C. 3470: *Greco: "Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche"*, 2 December 2015, http://www.camera.it/leg17/126?tab=&leg=17&idDocumento=3470.

[162] Stefania Maurizi, "Riecco il trojan di Stato: sulla cybersicurezza una partita di potere", in L'Espresso, 26 January 2016, http://espresso.repubblica.it/palazzo/2016/01/26/news/riecco-il-trojan-di-stato-sulla-cybersicurezza-una-partita-di-potere-1.247718.

[163] Italian Senate, Government bill: *Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*, http://www.senato.it/leg/17/BGT/Schede/Ddliter/46014.htm.

[164] In Italy, interceptions that are called "environment interception" or "interception between present people" are those occurring when microphones or cameras are hidden and used to record a crime.

[165] Italian Senate, Government bill: *Modifiche al codice penale e al codice di procedura penale*, cit., http://www.senato.it/service/PDF/PDFServer/BGT/00939937.pdf. See also Carola Frediani, "Le intercettazioni coi trojan arrivano in Parlamento: ecco cosa prevedono", in *La Stampa*, 5 August 2016, http://www.lastampa.it/2016/08/05/italia/politica/le-intercettazioni-coi-trojan-arrivano-in-parlamento-ecco-cosa-prevedono-VYJ5k6wkfoS8EkXL8iuqII/pagina.html.

ISSN 2280-6164

3.1.4 Wrap-up

Although a full and a comprehensive analysis of the procedures and techniques related to the collection of digital evidence within Italian jurisdiction is beyond the scope of the present work, it is, however, important to briefly mention some of its key aspects that emerged from the review of the existing literature and further interviews with key stakeholders.[166] In particular, the validity of the current legal framework, security concerns deriving from the growing terrorist threat and the burgeoning diffusion of encryption systems to secure communications are among the most debated aspects influencing how criminals are being prosecuted.

Depending on the interlocutor, the CPP is either considered a valid instrument to prosecute crime in cyberspace or not. For some, the Code is an adequate resource providing sufficient legal foundation for all actors and situations concerned in criminal proceedings. The 2008 law ratifying the Budapest Convention on Cybercrime[167] brought important modifications to Italian law, upgrading the CPP with satisfactory provisions to prosecute crime in cyberspace. In addition to setting up appropriate rules to carry out investigations when evidence is to be found in a digital format, the new provisions buttressed the need to ensure the integrity and originality of data during their acquisition and analysis, providing a framework of guarantees for the prosecuted.[168] On the other hand, other interviewed actors deplored the absence of a clear definition of the role of the forensic expert in Italian legislation, and suggested how some measures are used to impair the results of the technical analysis.

The recent wave of terrorist attacks across Europe and investigative hurdles followed by the widespread adoption of encryption tools by providers seem to be the two main drivers behind the approval of certain Italian regulations that some argue could restrict civil liberties. To fight serious crime and terrorism, retention terms have been prolonged and operators will have to store data until the end of June 2017. Similarly, various attempts to introduce the Trojan as a legitimate tool to collect evidence mainly derive from concerns associated with terrorism. In the last two years, only the 2016 reform of the CPP, which is evidently not a provision aimed at curbing terrorism or serious crime, tried to regulate the use of malware in investigations outside the broader context of the fight against terrorism. Though, a full of understanding of privacy and technical implications stemming from the use of the Trojan in Italy is not the primary objective of this paper, it is important to realize that the time seems ripe for full regulation of an issue that cannot continue

[166] For further reference see Andrea Ghirardini and Gabriele Faggioli, *Digital Forensics*, new ed., Milano, Apogeo, 2013. See also Giuseppe Vaciago, *Digital evidence. I mezzi di ricerca della prova digitale nel procedimento penale e le garanzie dell'indagato*, Torino, Giappichelli, 2012.

[167] Law No. 48 of 18 March 2008: *Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2008-03-18;48.

[168] Interviews, Rome, September 2016.

ISSN 2280-6164

to receive "legislative cover" by some articles of the CPP which are ill-suited for such a task.[169] According to some, the two contrasting verdicts of the Supreme Court would never have seen the light had the legislator intervened in a timely manner.[170] Proper regulation of the Trojan appear to be paramount given the long list of issues the legislator would need to standardize, possibly aiming to hold back from abusing a potentially powerful investigative tool that runs the risk of infringing of privacy.[171]

Italian law enforcement agencies have deployed (reportedly with parsimony) advanced tools to regain some of the investigative power they had lost with the spread of encryption to secure communications. In the past, police authorities had ample opportunities to investigate crime when criminals predominantly employed their mobile phone as a tool to communicate. Nowadays, however, as more and more criminals rely on information communication technologies (ICTs) using encrypted communication, police authorities feel they cannot adequately prevent and prosecute crimes if providers do not cooperate. Indeed, one should note that the Italian Electronic Communications Code asks operators to assist judicial authorities by providing "compulsory services," which include delivery of data and interception of communication upon request. As OTT service providers such as Google, Facebook, and Dropbox do not have to deliver these services, chances of effectively prosecuting crimes in cyberspace have dwindled.

This section briefly presented and analyzed the collection of evidence within Italian jurisdiction. Nevertheless, as data sought by enforcement agencies are increasingly stored abroad rather than immured within Italian borders, international cooperation between countries is becoming increasingly crucial. The next section explains how judicial cooperation between Italian and foreign authorities occurs in relation to the exchange of digital evidence.

3.2 Cross border requests and international cooperation in e-evidence gathering

Italian judicial authorities shall resort to Mutual Legal Assistance Treaties (MLATs), which Italy signs on a bilateral basis or in multilateral conventions, to obtain data stored abroad. Judicial assistance between Italy and foreign countries is regulated

[169] Ibid.

[170] Ibid.

[171] The main risks that were cited during interviews with experts were: the ability of the trojan of taking full control of the infected device; the possibility of recording through the microphone and the video-camera of the device; the possibility of transferring all the content stored in the device outside it; the ability to modify or add any file on the infected device; the difficulty to understand if the malware had infected the device and how; the question of who performed the technical operation (whether the judicial authority or a third party), and where and how the data collected will be stored.

ISSN 2280-6164

by the Constitution (art. 10), the CPP (Libro XI, titolo III),[172] international conventions and public international law. As of September 2016, Italy has some form of judicial assistance with 65 countries worldwide.[173] This section describes and evaluates how MLATs function when Italian authorities make requests of assistance to obtain digital evidence, focusing on the procedures in place between Italy and the USA and between Italy and EU member states. This section also introduces the analysis of a new legal instrument that Italian authorities may use when they seek to collect data stored abroad: the new article 234bis of the CPP.

3.2.1 Cooperation with the USA

International judicial cooperation between Italy and the USA on digital evidence and cross border data requests is crucial; being US based the main service providers and thus likely to store the majority of the data Italian authorities look for when pursuing criminals. Judicial cooperation between Rome and Washington is based on the Treaty on Mutual Assistance in Criminal Matters, which was signed in Rome in 2006.[174] Nearly half of the requests on judicial cooperation between the two countries entail digital evidence. In the last 3 to 4 years, Italy sent approximately 300 of these requests, with Facebook being the main provider to whom these requests were directed. Timing of MLATs procedures can vary substantially, ranging from some months to slightly less than a year.[175] According to the type of data Italian authorities intend to gather, procedures tend to vary. Usually, the more "invasive" the data requested, the harder and longer the process to obtain it becomes.

If *generic subscriber data* are sought – name, address and phone number; email address, payment method, but also access logs such as date, time and IP address of log-in – the main service providers normally accept requests from Italian authorities without resorting to the MLAT process. Nonetheless, because of the Electronic Communications Privacy Act (ECPA), American service providers are not compelled to hand over these data, and do so on a voluntary basis.[176]

In case of *traffic data* – sender and receiver, including IP addresses; date and time of communication, duration and "size" of communication; in case of emails, everything but the content – Italian authorities need to follow the MLAT process.

[172] Article 723 CPP; articles 201-206 (*norme di attuazione*) CPP.

[173] For a list of countries, see the Italian Ministry of Justice website: *Atti Internazionali*, updated 10 July 2014, https://www.giustizia.it/giustizia/it/mg_1_3.page?tabaip=y.

[174] Treaty between the United States of America and the italian Republic on Mutual Assistance in Criminal Matters, Rome, 3 May 2006, http://itra.esteri.it/vwPdf/wfrmRenderPdf.aspx?ID=49019.

[175] This finding is in line with the US President's Review Group on Intelligence and Communications Technologies, which maintains that the United States produce evidence to be delivered to its foreign partners on an average length of 10 months. See Richard A. Clarke et al., *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, 12 December 2013, p. 227, https://www.whitehouse.gov/blog/2013/12/18/liberty-and-security-changing-world.

[176] Interview, Rome, September 2016.

ISSN 2280-6164

There are important legal standards Italian authorities must meet: they have to show "specific and clear facts" proving a "probable cause" that the sought data is relevant for the ongoing criminal investigation. These legal standards, which need to be satisfied in order to make service providers produce such evidence, derive from the ECPA.[177]

In case of *content data*, Italian authorities start the MLAT process and send their request to the US Department of Justice, which redirects it to the US attorney's office with jurisdiction. There, it is evaluated by the Assistant US Attorney, who formulates a request, motivated by an affidavit of a federal agent, to be presented to a federal judge. If the federal judge ascertains that a "probable cause" exists, it authorizes the search warrant. In this context, "probable cause" means that the account should contain the evidence of the crime: Italian authorities have to precisely describe the facts that make probable the presence of the criminal evidence in the account of the person being investigated. The prosecutor later forwards the search warrant to the ISP, which usually produces the digital evidence in CD format. The entire process traces its roots back to the IV amendment.[178]

In case of terrorism or non-terrorism episodes implying a death threat or kidnappings, essentially when there is no time to initiate the MLAT process, US authorities can facilitate Italian authorities with "emergency voluntary requests." In these situations, the legal attaché at the United States Embassy in Rome should be contacted.[179]

It is worth noticing that in the United States, service providers are not compelled to retain data, although ECPA requires *data preservation* for up to 90 days, which can be prolonged for another 90 days, upon request by the prosecutor.[180] Generally, the main providers preserve data for longer periods, if foreign authorities need to obtain them through MLAT. Hence, service providers will retain data until the requested date, at the end of which they are erased, unless they are kept by the providers for purposes other than the investigation. The main service providers

[177] See U.S. Code, title 18, part I, sec. 2703(d), https://www.law.cornell.edu/uscode/text/18/2703. Interview, Rome, September 2016.

[178] See U.S. Constitution Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Interview, Rome, September 2016.

[179] Interview, Rome, September 2016.

[180] See U.S. Code, title 18, part I, sec. 2703(a), "A Governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." See also Kristina Ringland, "The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model", in *Shidler Journal of Law, Commerce, and Technology*, Vol. 5, No. 3 (2009), http://hdl.handle.net/1773.1/427.

ISSN 2280-6164

generally accept requests from foreign authorities to retain data without the need for the MLAT.[181]

3.2.2 Cooperation with EU member states

As for France and Germany, Italy has adopted the following conventions and agreements relevant for cooperation on criminal matters across Europe: the European Convention on Mutual Assistance in Criminal Matters (ECMACM), parts of the Schengen agreement, the European Convention on Mutual Assistance in Criminal Matters[182] and its Protocol[183] and the Convention on Cybercrime. Moreover, the European Investigation Order (EIO) will have to be transposed into Italian legislation by May 2017.

Interestingly, a recent memorandum issued by the Ministry of Justice in August 2015 underlined the tools provided by ECMACM (ratified with Law No. 215 of 23 February 1961) and the Schengen agreement (ratified with Law No. 388 of 30 September 1993) to Italian national authorities when they request judicial assistance to foreign authorities.[184] Citing the increasing number of requests the Ministry has to process, the memorandum argues that the two conventions allow Italian judges to directly ask for assistance from their foreign peers, thus eliminating the need to receive the political approval for sending the request.[185] The memorandum also maintains that direct contact between judicial authorities should be preferred, as opposed to involving the Ministry of Justice, which instead should be dealing with MLATs requiring the Ministry and diplomatic approval.[186]

Despite having ratified the European Convention on Mutual Assistance in Criminal Matters, Italy has not yet implemented it. Therefore, judicial cooperation with other EU member states mainly relies on ECMACM. Problems regarding its implementation seem to revolve around cultural challenges to adopting more

[181] Interview, Rome, September 2016.

[182] Council of the European Union, *Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member states of the European Union*, cit.

[183] Council of the European Union, *Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union*, 16 October 2001, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:42001A1121(01).

[184] Italian Ministry of Justice, *Circolare: Cooperazione giudiziaria internazionale in materia penale*, 10 August 2015, https://www.giustizia.it/giustizia/it/mg_1_8_1.page?contentId=SDC1217132.

[185] Indeed, the memorandum argues that, according to article 15 of the ECMACM, in case of urgency, Italian judicial authority can directly send a rogatory to foreign authorities, adding that also requests of "pre-trial investigations" (*indagini preliminari*) can occur through direct contact between judicial authorities. The memorandum emphasizes its argument noting that, since the entry into force of the Schengen agreement, direct transmission between judicial authorities have become the main channel to send a rogatory, this without being limited to emergency situations or pre-trial investigations.

[186] Italian Ministry of Justice, *Circolare: Cooperazione giudiziaria internazionale in materia penale*, cit.

ISSN 2280-6164

frequent direct contacts between judicial authorities, the use of a common language and limited knowledge of EU member states' national jurisdictions.[187]

The collection and exchange of digital evidence in relation to cybercrime is simplified in the Convention on Cybercrime, which was signed in Budapest in 2001. As of September 2016, 49 countries have ratified the convention, whereas six others have only signed it. The Convention had been the first international agreement on cybercrime, whose adoption was driven by the need to coordinate criminal investigations on cybercrime across Europe. Article 25 of the Convention states that countries "shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data" and that in urgent circumstances may "make requests for mutual assistance or communications related thereto by expedited means of Communication."[188] In Italy, the Convention on Cybercrime was transposed with Law No. 48 of 18 March 2008. Its ratification commenced in May 2007, while the convention came into force on 5 April 2008. For the first time, the convention introduced specific criminal procedure provisions concerning the collection of digital evidence, modifying criminal procedure articles concerning search, seizure, acquisition and conservation of data stored in digital devices. The articles introduced with the Convention, and the subsequent modifications to criminal procedure law, were crucial to regulate key elements of digital evidence, above all the necessity to ensure its integrity, which was overlooked by a prior text elaborated by the Government.[189]

On 3 April 2014, the European Parliament and the Council approved Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters.[190] The provisions of the directive will have to be transposed in national jurisdictions of all EU member states by 22 May 2017. The directive provides a framework for EU member states' judicial authorities to "have one or several specific investigative measure(s) carried out in another Member State" in order to acquire evidence (art. 1(1)). Law enforcement agencies should use an EIO when it seems "proportionate, adequate and applicable" to the prosecuted crime (preamble). This includes also the interception of telecommunications, including their content and the "collection of traffic and location data associated with such telecommunications, allowing competent authorities to issue an EIO for the purpose of obtaining less intrusive data on telecommunications" (preamble). The interviewed officials suggested that transposition into Italian legislation should occur smoothly, as opposed to what happened with the European Convention on Mutual Assistance in Criminal

[187] Interview, Rome, October 2016.

[188] Council of Europe, *Convention on Cybercrime*, cit. See also Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, cit.

[189] Stefano Aterno, *Digital Forensics*, cit.

[190] Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in Criminal Matters, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32014L0041.

ISSN 2280-6164

Matters.[191]

3.2.3 A new legal measure to collect e-evidence abroad: article 234 bis

Of particular relevance for the collection of digital evidence abroad is the new article 234bis ("*Acquisizione di documenti e dati informatici*"), introduced in the CPP by Law No. 43 on 17 April 2015. The article states that the acquisition of documents and data stored abroad, even those not publicly available, is always allowed with the consent of the legitimate owner (*legittimo titolare*).[192] This article is remarkably similar to article 32 ("Trans-border access to stored computer data with consent or where publicly available") of the Budapest Convention on Cybercrime.[193] Interestingly, article 32 had not been incorporated into Italian CPP at the time of the Convention's ratification. As opposed to article 32 of the Convention, article 234bis refers to all crimes and not only to cybercrime.[194]

Some legal experts argue that, whereas the collection of publicly available data (for instance, public profiles on social networks, sites or blog content, posts on forums etc.) generally occurs without prior consent, thus indirectly confirming well-established investigation procedures and techniques, the acquisition of non-publicly available data (those accessible with authentication credentials or generally protected by cryptography), is more controversial, as it is not clear who the "legitimate owner" might be.[195] Not knowing who the legitimate owner is leaves nonetheless many doors open, especially considering that more than one subject could legitimately be asked to express consent on the data sought.[196] Pointing the Italian Privacy Code, some suggest that the legitimate owner could be identified with the so-called "data controller."[197] However, if the legislator sought to identify the legitimate owner with the data controller in article 234bis, the decision-maker

[191] Interview, Rome, October 2016.

[192] "È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare."

[193] "A Party may, without the authorisation of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or (b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." Council of Europe, *Convention on Cybercrime*, cit.

[194] Interview, Rome, September 2016. See Stefano Aterno, "L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella privacy", in *Archivio penale*, No. 1/2016 (January-April 2016).

[195] Ibid.

[196] Interview, Rome, September 2016.

[197] Defined in sec. 4(1) of the Personal Data Protection Code as "any natural or legal person, public administration, body, association or other entity that is competent, also jointly with another data controller, to determine purposes and methods of the processing of personal data and the relevant means, including security matters." See also Stefano Aterno, "L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella privacy", cit.

ISSN 2280-6164

would have clearly referenced the Privacy Code.[198] Another solution is to pinpoint the legitimate owner from the terms of contract users agree to when they start using service providers' services. In this case, if the contract foresees that the service provider is authorized to share user's data under certain conditions, the provider becomes the legitimate owner, and Italian authorities could eschew the activation of the MLAT procedure by directly requesting the data from the provider.[199]

As a practical example, in June 2015, during a case involving the suicide of a woman, the lawyer supervising the case requested, through article 234bis, to obtain data published on the public profile of a well-known service provider, whose account had been blocked by the woman before having committed suicide. The request was not accommodated and the provider declared it was not allowed to disclose such information without following the proper legal procedure.[200] A year after its introduction, it is not known whether the article has already been applied, so that it might be too early to assess its value-added in the obtainment of digital evidence outside Italian jurisdiction.[201]

3.2.4 Wrap-up

Cooperation between Italy and the USA on cross border data requests is considered to be working well, even though the long procedure required in requesting evidence from service providers has in part riddled the MLAT process. Data requests that seem to be working better than others are those in the context of "emergency voluntary requests," referring to emergency situations where Italian authorities do not have to undergo the MLAT process. Requests involving the activation of MLAT instead are delayed on both sides of the Atlantic. Interviewed experts notice that the entire process, from the formulation of the request by Italian authorities to the production of evidence by American providers, can take up to several months. On the Italian side, the formulation by Italian authorities of the request might take long in order to enhance the chances of meeting US legal standards of "probable cause." For example, in a case involving child pornography, Italian authorities requested all the chats of the investigated person to look for evidences of other pornography related-crimes. For US authorities, a search warrant can be issued only if the account of the prosecuted person contains evidence of a specific crime in order to avoid unjustified searches.[202] On the other hand, it is difficult for US authorities to keep up with the incessant pace of data requests coming not only from Italy, but also from the rest of the countries worldwide.[203] In order to speed up the process,

[198] Stefano Aterno, "L'acquisizione di dati personali tra misure antiterrorismo e intromissioni nella privacy", cit.
[199] Ibid.
[200] Interview, Rome, September 2016.
[201] Ibid.
[202] Interview, Rome, October 2016.
[203] Interview, Rome, September 2016.

ISSN 2280-6164

although it is not completely clear how and who should make such a decision, some suggest the need to prioritize the quality and the number of requests. Many of the experts interviewed would also welcome a cross border data accord between Rome and Washington, similar to the one agreed between the USA and the UK in July 2016. They are, however, also aware of the fact that it is easier for two countries with similar legal systems to match each other's judicial cooperation needs.[204] Nonetheless, it seems that the two countries' judicial authorities are considering reviewing the treaty on mutual assistance in order to speed up the process of digital evidence exchange.[205] Lastly, it is unclear what the consequences of the verdict of the US Second Circuit on the Microsoft Warrant Case, which ruled against the US Government, will produce. Following the sentence, providers suggested that they will no longer be able to hand over data to the Department of Justice if they are stored in servers overseas. According to the interviewed experts, Italian national authorities will have to redirect their requests to the countries where the data are stored. Department of Justice's petition to reopen the case leaves the situation uncertain.[206]

Despite the ample legislative framework, Italy and other EU member states still need to recur to MLATs to obtain digital evidence stored in servers located on their territories. Only the Convention on Cybercrime cites "expedited measures" for the collection and exchange of evidence, but this evidence is restricted to cybercrime and has not been signed by all member states. The great majority of the Italian experts interviewed would indeed auspice a harmonization of the procedures regarding the collection, preservation and exchange of digital evidence between members of the EU. However, many of them notice that such a harmonization would not easy to achieve, as member states have different legal traditions, including rather discrete criminal procedure laws.[207] Moreover, Italian experts and officials notice that cross border data requests between EU member states are minimal compared to those sent overseas, somehow implying that regulating the issue of data requests uniquely at the EU level without involving major third countries and providers would do little to solve this much more complex puzzle.[208]

Finally, despite the possibilities allowed by the vagueness of its language, article 234bis offers an example of the intrinsic limits of the current status quo regarding international cross border data requests. Although the article would theoretically allow for the disclosure of data by providers, they cannot be compelled to produce such evidence and, even when conditions would allow it, they would be wary to perform such an activity to avoid abusing users' privacy. In addition, some have commented that a direct request made by law enforcement authorities to providers,

[204] Ibid.

[205] Interview, Rome, October 2016.

[206] Charlie Osborne, "US Strikes Back in Microsoft Email Warrant Case", in *ZDNet*, 17 October 2016, http://zd.net/2easfer.

[207] Interview, Rome, September 2016.

[208] Interview, Rome, October 2016.

ISSN 2280-6164

especially in relation to certain data, would be seen as a violation of MLATs, rather than a valid alternative to obtaining digital evidence stored abroad.[209]

ISSN 2280-6164

[209] Interview, Rome, September 2016.

4. E-evidence in the European Union

by Simona Autolitano[210]

In the digital age, where information technologies have been expanding in nearly every sector of our society,[211] obtaining electronic evidence has become an essential activity to fight cross-border crime.[212] It is not by chance, hence, that the Council of the European Union has recently stressed the importance of gathering e-evidence to be used in criminal proceedings for all types of crime.[213] The principle of mutual recognition is becoming a key element in European cooperation on criminal matters and the recent approval of the European Investigation Order (EIO) represents a significant step forward.[214] Nevertheless, for the purpose of electronic evidence, the Directive still does not solve the problem of its collection and exchange. As a result, mutual legal assistance (MLA) procedures remain the main mechanism by which the European Union's member states exchange digital evidence. Combating cross-border crime and terrorism should be a common European responsibility.[215] The European Union is increasingly enhancing police and judicial cooperation in criminal matters, gradually covering different aspects of pre- and post-trial measures, to reach a certain degree of harmonisation in criminal procedures across member states.[216] Founding documents for obtaining criminal evidence across EU member states are the Council of Europe Convention on Mutual Assistance in Criminal Matters,[217] the Schengen Convention,[218] the European Convention on Mutual Assistance in Criminal Matters and its Protocols.[219]

[210] Simona Autolitano is intern at the Istituto Affari Internazionali (IAI).

[211] John Arquilla and David Ronfeldt, "Cyberwar is Coming!", in John Arquilla and David Ronfeldt (eds.), *Athena's Camp. Preparing for Conflict in the Information Age*, Santa Monica, Rand Corporation, 1997, p. 41, http://www.rand.org/pubs/monograph_reports/MR880.html.

[212] Council of the European Union, *Council Conclusions on Improving Criminal Justice in Cyberspace*, cit.

[213] Ibid.

[214] Council of the European Union, *Tampere European Council Presidency Conclusions*, 16 October 1999, http://www.europarl.europa.eu/summits/tam_en.htm.

[215] Jean-Claude Juncker, *A New Start for Europe*, cit.

[216] Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, cit.

[217] Council of Europe, *The European Convention on Mutual Assistance in Criminal Matters*, cit.

[218] Council of the European Union, *Council Decision Concerning the Definition of the Schengen Acquis*, 20 May 1999, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:31999D0435.

[219] Council of the European Union, *Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member states of the European Union*, cit.

ISSN 2280-6164

4.1 Judicial cooperation in criminal matters in the European Union

Traditionally based on the mutual legal assistance (MLA) procedures, the current legal framework in the field of European judicial cooperation is moving towards the principle of "mutual recognition," identified as the "cornerstone" of the future development of European judicial cooperation.[220] Originally introduced by the Court of Justice of the European Union (CJEU) in 1979 to foster the creation of the Single Market, the principle has been the engine of European integration in criminal matters.[221] According to this principle:

> once a certain measure, such as a decision taken by a judge in exercising his or her official powers in one Member State, has been taken, that measure [...] would automatically be accepted in all other member states, and have the same or at least similar effects there.[222]

In other words, based on mutual trust and confidence, each member state recognises the validity of other member states' courts decisions. Ultimately, the principle of "mutual recognition" aims to replace traditional forms of international cooperation,[223] considered slow, cumbersome and uncertain.[224] The EU has concretely applied for the first principle with the adoption of the European Arrest Warrant (EAW) in 2002.[225] Based on a high level of confidence between member states, the EAW aimed at replacing the system of multilateral extradition with faster and simpler surrender procedures. For this reason, the EAW represents a major landmark for the development of the principle of "mutual recognition" in criminal law.

Police and judicial cooperation in the EU developed in 1985 with the creation of the Schengen area. By abolishing checks at its internal borders, the EU became aware of the need of effectively pursue criminals acting across European countries and envisaged a series of judicial procedures to facilitate and accelerate investigations in criminal matters. The Schengen acquis[226] has introduced, for instance, a large-

[220] European Commission, *Mutual Recognition of Final Decisions in Criminal Matters* (COM/2000/495), 26 July 2000, p. 3, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:52000DC0495.

[221] Valsamis Mitsilegas, *EU Criminal Law*, Oxford and Portland, Hart, 2009.

[222] European Commission, *Mutual Recognition of Final Decisions in Criminal Matters*, cit., p. 2.

[223] Mutual legal assistance procedures, usually based on MLATs, represents the most common way to foster international judicial cooperation. See Jordan L. Paust et al., *International Criminal Law. Cases and Materials*, Durham, Carolina Academic Press, 2000.

[224] Ibid.

[225] Council of the European Union, *Council Framework Decision on the European Arrest Warrant*, Brussels, 13 June 2002, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32002F0584.

[226] The Schengen acquis results from the Schengen Agreement initially signed in 1985 by five member states and gradually extended to other EU and non-EU countries, including Iceland, Norway and Switzerland. Created outside the European legal framework, it has been integrated into

ISSN 2280-6164

scale information sharing system, the so-called Schengen Information System (SIS), to improve efficiency in the fight against serious and organised crime (SOC).[227] Furthermore, in some cases, cross-border surveillance could have been authorised to facilitate the collection of data across European countries.[228] Interestingly, the Schengen Convention highlighted the relevance of pre-trial measures in judicial cooperation stating that "data on objects sought for the purposes of seizure or use as evidence in criminal proceedings shall be entered in the Schengen information system."[229]

Based on the principles and guidelines of the Council of Europe Convention of 20 April 1959 and its protocols, the European Convention on Mutual Assistance in Criminal Matters of 29 May 2000 represents a first concrete step towards the creation of a European "governance" in the field of judicial cooperation, including evidence-gathering. In drawing up the 2000 Convention, the Council has supplemented the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its 1978 Protocol, as well as the Convention of 14 June 1990 implementing the Schengen Agreement.[230] The Convention regulates relevant points stemming from the widespread use of new technologies, including the interception of telecommunications (art. 17-22), which may be either intercepted and transmitted directly to the requesting State or recorded for subsequent transmission. Furthermore, it also put forward the "spontaneous exchange of information" (art. 7), according to which, without the need for a mutual assistance request, competent authorities are allowed to exchange information concerning criminal offences covered by article 3 of the Convention. The "spontaneous exchange of information" denotes an improvement of the judicial cooperation in criminal matters, usually based on the "request principle;" namely, law enforcement authorities were not allowed to disclose any information without having previously received a formal mutual assistance request.[231]

Beyond information exchange, judicial cooperation encompasses pre-trial orders, namely those measures "concerning the recognition of decisions on the freezing of evidence."[232] In 2002, following the Council's guidelines on implementing mutual

the legal framework of the European Union by the Treaty of Amsterdam, which came into effect in May 1999. The Schengen acquis includes all the provisions and decisions implementing the former Schengen Agreement, thus establishing the so-called Schengen area. For a detailed list of provisions, see Council of the European Union, *The Schengen Acquis Integrated in the European Union*, Luxembourg, Office for Official Publications of the European Communities, 2001, http://bookshop.europa.eu/en/-pbBX2699651/.

[227] The system was replaced in 2006 with the second generation Schengen Information System (SIS II).

[228] Council of the European Union, *The Schengen Acquis Integrated in the European Union*, cit., p. 40.

[229] Ibid., p. 72.

[230] Council of the European Union, *Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member states of the European Union*, cit.

[231] Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, cit.

[232] Council of the European Union, *Programme of Measures to Implement the Principle of Mutual*

ISSN 2280-6164

recognition, important steps forward have been made in the field of collection and exchange of evidence. Following the adoption of the already mentioned EAW, the 2003 Council Framework Decision on the execution in the EU of orders freezing property or evidence and the 2008 Council Framework Decision on the European Evidence Warrant (EEW) have been included in the EU legislative framework to govern the sensitive topic of cross-border gathering and use of evidence in criminal proceedings.[233] However, despite the undisputable role of digital means in fostering criminal activities, electronic evidence does not fall either under the umbrella of the EEW nor under the 2003 Council Framework Decision on the freezing of evidence.

Interestingly, and in spite of not being an EU institution, the Council of Europe has been the first to address the potential challenges concerning evidence in cyberspace for police and judicial cooperation with the adoption of the 2001 Budapest Convention.[234] The Convention tries to address problems of criminal procedural law connected with information technologies, thus providing a legal framework to ensure the collection of evidence in cyberspace. In urgent cases, "expedited means of communication, including fax or e-mail" have been conceived to accelerate the process of evidence-gathering (art. 25(3)). More importantly, specific provisions authorise "expedited preservation of stored computer data" before that an actual request for mutual assistance has been formally submitted (art. 29). Interestingly, the Convention governs also cases of mutual assistance concerning the access to stored computer data "located within the territory of the requested Party" (art. 31(1)), thus allowing "trans-border access to stored computer data with consent or where publicly available" (art. 32); namely, under certain conditions, an authority in the issuing country may access or receive, through a computer system in its territory, stored computer data located in the territory of another State Party to the Convention. In order to foster judicial cooperation in criminal matters, the Convention has also provided the setting up of a 24/7 Network, according to which each "point of contact [should be] available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings" (art. 35(1)). In addition, the "production order" (art. 18) represents also an important measure authorised by the Convention as it covers the enforceability of domestic production orders outside the territory such as "to submit specified computer data [...] stored in a computer system" (art. 18(1)). Nevertheless, the Budapest Convention, to date ratified by 49 parties, including 25 out of 28 EU member states, remains limited in its scope as it applies only to cybercrime.

Recognition of Decisions in Criminal Matters, 15 January 2001, p. 14, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32001Y0115(02).

[233] Council of the European Union, *Council Framework Decision 2003/577/JHA on the Execution in the European Union of Orders Freezing Property or Evidence*, 22 July 2003, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32003F0577.

[234] Council of Europe, *Convention on Cybercrime*, cit.

ISSN 2280-6164

In order to ensure the collection and exchange of digital evidence, it is necessary that telecommunications and internet service providers make those data available for law enforcement activities. After the Madrid bombings in 2004, the EU realised the importance of controlling this field.[235] Seeking to harmonize member states' provisions on data retention, the EU adopted in March 2006 the well-known Data Retention Directive.[236] Firstly, it applies to the "providers of publicly available electronic communications services or of a public communications network" (art. 3) only for certain data – subscriber and traffic data (art. 5). The data retention period was left to member states' respecting however a minimum of six months and a maximum of two years (art. 5). Finally, those data should have been used exclusively for the purpose of "prevention, investigation, detection and prosecution" of serious and organized crime (preamble). Despite the importance of data retention for "general interest, namely [...] public security," in April 2014, the Court of Justice of the European Union (CJEU) invalidated the directive in view of the already mentioned right to "private life" and right to the protection of personal data of individuals.[237] According to the Court, the indiscriminate retention of data of "both legal entities and natural persons," would have constituted a constant surveillance, direct in contrast with the right to privacy. As clearly stated by the Commission, the EU has no intentions to further legislate on the field.[238] Member states, acting via the Council of the EU, are in a standoff with the European Commission, having invited it to present a new legislative initiative on bulk electronic communication data retention whenever possible,[239] despite the Commission's stated objections to doing so, preferring to remain a neutral observer of member states' domestic legislative efforts in this area.[240]

While enhancing criminal justice, the EU has recognised the importance of upholding human rights and the rule of law in cyberspace.[241] Human rights are at the forefront of the EU's action;[242] deriving from a solid tradition, rooted in

[235] Council of the European Union, *Declaration on Combating Terrorism*, Brussels, 25 March 2004, http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf.

[236] 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, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32006L0024.

[237] Court of Justice of the European Union, *Judgement of the Court in Joined Cases C-293/12 and C-594/12*, cit.; *The Court of Justice declares the Data Retention Directive to be invalid*, 8 April 2014, p. 2, http://curia.europa.eu/jcms/jcms/P_125951.

[238] European Commission, *Statement on National Data Retention Laws*, 16 September 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5654_en.htm.

[239] Council of the European Union, *Outcome of the 3433rd Council Meeting Justice and Home Affairs*, Brussels, 3 and 4 December 2015, p. 6, http://www.consilium.europa.eu/en/meetings/jha/2015/12/03-04.

[240] Statewatch, *Data retention: Commission Still Refusing Demands for New Mass Surveillance Measures*, 17 March 2016, http://www.statewatch.org/news/2016/mar/data-retention-com-pressure.htm.

[241] Council of the European Union, *Council Conclusions on Improving Criminal Justice in Cyberspace*, cit.

[242] "Fundamental rights [...] shall constitute general principles of the Union's law." See

ISSN 2280-6164

the Council of Europe Human Rights Convention (ECHR) and the EU Charter of Fundamental Rights.[243] One of the EU's fundamental pillars is the right to "private life," recognised in the article 7 of the Charter. Cyberspace constitutes a huge challenge for the protection of personal data and the actual application of human rights.[244] Considering the need to adapt the EU legislation on data protection to new technologies and related cyber challenges, the EU has carried out an extensive reform package to ensure the protection of personal data in the digital age.[245]

Three important reforms of data protection rules have been put forward. The General Data Protection Regulation (GDPR),[246] which replaces the previous Data Protection Directive,[247] aims to make "data protection fit for the digital age."[248] Entered into force in May 2016, the GDPR shall apply from 25 May 2018. It ensures a high level of protection of personal data and regulates the transfer of personal data for commercial purposes. Users and businesses will both benefit from the new regulation. Citizens' will have more information on the transfer of their personal data, companies will rely on clearer provisions, which will apply also to non-EU businesses, offering services to EU costumers.

As the GDPR does not apply to certain activities – among others, personal data processed by public authorities in the course of criminal investigations[249] – it has been complemented by the Criminal Law Enforcement Data Protection Directive, which applies specifically to the processing of personal data in the police and judicial sector.[250] The "Police Directive" will ensure the protection of personal data

article 6 of the Treaty on European Union, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=OJ:C:2016:202:TOC.

243 The Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, has the same legal value as the Treaties.

244 Nikolas Ott and Hugo Zylberberg, "A European Perspective on the Protection of Personal Data in Cyberspace", in *Kennedy School Review*, 14 September 2016, http://harvardkennedyschoolreview.com/?p=3958.

245 Věra Jourová, "How will the EU's reform adapt data protection rules to new technological developments?", in *European Commission Factsheets*, January 2016, http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_technological_developments_2016_en.pdf.

246 Regulation (EU) 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32016R0679.

247 Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:31995L0046.

248 European Parliament, *Data Protection Reform: Parliament Approves New Rules Fit for the Digital Era*, Strasbourg, 14 April 2016, http://www.europarl.europa.eu/news/en/news-room/20160407IPR21776.

249 Preamble, para. 19, Regulation (EU) 2016/679, cit.

250 Directive (EU) 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, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32016L0680.

ISSN 2280-6164

transferred for the purpose of evidence in criminal investigations. It lays down specific rules for the exchange of data in the field of prevention, investigation, detection and prosecution of criminal offences, as well as execution of criminal penalties. When competent authorities deal with different tasks than those just mentioned, the transfer of data falls within the scope of the Regulation.[251] The Directive does not consider police and judicial cooperation with third countries, as it applies only to those data transmitted or made available between member states. In this case, member states remain able to enforce bilateral agreements for the transfer of data in criminal proceedings.[252]

For some other activities, the transfer of data follows neither the GDPR nor the Police Directive. Specifically, any activities concerning national security such as "activities of agencies or units dealing with national security issues," remain outside the scope of both the legislative measures.[253] The same applies for the processing carried out by "a natural person in the course of a purely personal or household activity."[254] In those cases, member states shall apply national rules.

With the GDPR and Police Directive in place, the EU is now turning its attention to reform of the Directive on Privacy and Electronic Communications (ePrivacy Directive).[255] This Directive sets out a strong prohibition on the interception and recording of certain electronic communications, and the retention of associated metadata for those communications (e.g. call histories). Article 15 of the ePrivacy Directive sets out the limits on the EU and member states' discretion to derogate from those obligations for law enforcement purposes – including the (now invalidated) Data Retention Directive.[256] Reform of the ePrivacy Directive – prompted by a need to update it and align it with the new GDPR – will therefore be a central part of the EU's consideration of acceptable interferences with online privacy in the name of law enforcement and public security.

The few existing EU legal instruments show a fragmented EU legal framework in the field of judicial cooperation in criminal matters,[257] even though the 2010 Stockholm Programme clearly highlighted the need for a comprehensive and more systematic cooperation in criminal matters.[258] Against this backdrop, the

[251] Preamble, para. 19, Regulation (EU) 2016/679, cit.

[252] Directive (EU) 2016/680, cit.

[253] Preamble, para. 14, ibid.; article 2, Regulation (EU) 2016/679, cit.

[254] Article 2, Regulation (EU) 2016/679, cit.

[255] Directive 2002/58/EC of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.

[256] Court of Justice of the European Union, *Judgement of the Court in Joined Cases C-293/12 and C-594/12*, cit.

[257] See Preamble, para. 5, Directive 2014/41/EU, cit.

[258] European Council, *The Stockholm Programme. An Open and Secure Europe Serving and Protecting Citizens*, 4 May 2010, http://eur-lex.europa.eu/legal-content/en/

ISSN 2280-6164

European Investigation Order (EIO) Directive,[259] expected to be transposed into member states' legal framework by May 2017, inserts itself in this context as a new instrument, aiming to further facilitate judicial cooperation in criminal matters (preamble, para. 7). Ultimately, the goal of the EIO is to replace most of the existing instruments in this area, thus moving from a mutual legal assistance to a mutual recognition principle. Nevertheless, it should be noted that the territorial scope of the Directive remains limited; indeed, not all EU member states agreed upon the implementation of the EIO. While the UK has opted-in, Ireland and Denmark decided to remain outside the scope of the EIO. As a consequence, the EIO cannot replace all the existing instruments for all countries and so the previous framework remains in play. By clearly stating that member states must execute the EIO on the basis of the principle of mutual recognition (art. 9(1)), the EIO Directive can be seen as the first major instrument on mutual recognition adopted since the entry into force of the Lisbon Treaty.

Two major parts of the EIO Directive can be identified. The first section, which includes Chapters I-III, deals with general rules underpinning the application of the principle of mutual recognition in the field of collection and exchange of criminal evidence. The second section, Chapters IV-VI, contains specific provisions for certain investigative measures; for instance, on the temporary transfer of evidence (art. 22), hearing by videoconference (art. 24), information on banking and other financial operations (art. 26), covert investigations (art. 29) and interceptions (art. 30, 31). According to the Directive, a State can issue an EIO regarding one or several specific investigative measures, which should be carried out in another member state, including the exchange of evidence, if available in the executing State (art. 1(1)). The EIO includes the collection or transfer of e-evidence, here conceived exclusively as electronic data obtained from interception of telecommunications (ch. V). The chapter that is dedicated to this kind of electronic evidence, clarifies that the term "data" refers not only to "the content of the telecommunications, but could also cover collection of traffic and location data associated with such telecommunications" (preamble, para. 30). As the EIO does not take into account the collection or exchange of digital evidence not obtained from interception, no references on data retention have been made. Mandatory deadlines for recognition or execution have been also included, aiming at enhancing efficiency of judicial cooperation. It is noteworthy that although EIOs are mandatory for receiving authorities, the EIO Directive does not *require* that authorities seeking data from other member states use the EIO framework to make the request in the first place. The decision on the recognition or execution of a EIO must be taken in principle no later than "30 days after the receipt of the EIO" (art. 12(3)), while investigations should be carried out by the executing authority "not later than 90 days" (art. 12(4));" however, a shorter deadline can be negotiated in case of urgency, e.g. seriousness of the offence. Finally, grounds for refusal have been clearly listed in article 11, where in addition to traditional restrictions, such as immunity or privilege and

TXT/?uri=celex:52010XG0504(01).

[259] Directive 2014/41/EU, cit.

ISSN 2280-6164

incompatibility with the executing State's obligations, concerns for "national security interests" have been listed. Interestingly, the 1959 Convention included such an undefined cause, allowing the requested party to refuse to cooperate if it "considers that execution of the request is likely to prejudice the sovereignty, security, [public order] or other essential interests of its country."[260]

In conclusion, the EU has put forward a series of instruments to enhance judicial cooperation in criminal matters. In this sense, the principle of mutual recognition has been the main driver of judicial cooperation within European borders.[261] As mentioned, the advantages of the "mutual recognition" principle rely on mutual trust and confidence over one another's legal systems so that judicial decisions can be enforced much more quickly and with greater certainty.[262] For the purposes of securing and obtaining evidence, the EIO represents a significant leap forward on two fronts; on the one hand, it creates a harmonized instrument regulating the collection and exchange of evidence, including data stemming from interceptions of telecommunications; on the other hand, it represents an important landmark for the development of the principle of "mutual recognition," albeit not in every cross-border scenario in which interceptions may be needed – for instance where the executing State is Ireland or Denmark.

The European Union's attempt to systematise evidence-gathering with the adoption of the EIO represents a significant advancement, but it will not deliver full harmonization for the collection and the exchange of digital evidence for criminal investigations. Investigative powers and rules of criminal procedure, even among countries with similar legal traditions, will still differ considerably. Thus, it could happen that electronic evidence, obtained according to the rules of one legal system is not suited to form a reliable basis for decision in another EU legal system. Without a comprehensive European legal framework, which defines specific standards on procedures and modalities for the collection and exchange of electronic evidence, member states tend to act differently, often deciding on a case-by-case basis.[263] Therefore, obtaining e-evidence remains primarily governed by national law and national criminal procedural provisions.[264]

In such a composite picture, the 2001 Convention on Cybercrime remains the leading international legal framework for prosecuting cybercrime.[265] With its provisions authorising expeditious action, the Convention can in some case offer a "fast and effective regime" or international criminal justice, thus responding to the problem of the collection of electronic evidence. Undoubtedly, the Budapest

[260] See Article 2b. Council of Europe, *The European Convention on Mutual Assistance in Criminal Matters*, cit.
[261] Council of the European Union, *Tampere European Council Presidency Conclusions*, cit.
[262] Ibid.
[263] Ibid.
[264] Ibid.
[265] Council of Europe, *Convention on Cybercrime*, cit.

ISSN 2280-6164

Convention, which provides law enforcement powers to secure computer data in specific criminal investigations, has contributed to enhance cooperation in the fight against cybercrime. The treaty puts forward information sharing among signatory countries and entrusts internet service providers (ISPs) with the task of capturing and retaining communications data for use in criminal investigations (art. 18). However, as mentioned, it is limited in its scope, as it applies only to evidence leading to conviction of computer-related crimes. Further, relying for the most part on MLA, rather than mutual recognition or permitted direct trans-border access, it has been criticized as "inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned."[266] Therefore, evidence-gathering in cyberspace, even within European borders, is still rather dependent on voluntary cooperation between authorities, or, when gathered evidence needs to be legally admissible or if a coercive measure is required, on cumbersome MLA procedures.[267]

4.2 Judicial cooperation and "digital relations" with the United States

In the digital age, however, the fight against cross-border crime cannot be limited to European borders. As a result, the EU is creating solid cooperation channels with third countries such as the United States. Concerning evidence-gathering, in February 2010, the US-EU framework agreement[268] entered into force, to facilitate the collection and exchange of information in criminal matters.[269] Among the most important innovations can be mentioned the "identification of bank information" (art. 4), the setup of "joint investigative teams" (art. 5) and the "expedited transmission of requests" (art. 7).[270] One of the major obstacles for EU-US cooperation relies on different understandings of criminal offences,[271] the problem

[266] Cybercrime Convention Committee, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, Strasbourg, Council of Europe, 3 December 2014, p. 123, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c.

[267] European Commission Community Research and Development Information Service (CORDIS), *EVIDENCE Report Summary*, last updated 6 April 2016, http://cordis.europa.eu/result/rcn/181783_en.html.

[268] Agreement on Mutual Legal Assistance between the European Union and the United States of America, Washington, 25 June 2003, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=5441.

[269] Council of the European Union, *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*, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=celex:32009D0820.

[270] Sergio Carrera et al., *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, Brussels, Centre for European Policy Studies (CEPS), 2015, p. 46, https://www.ceps.eu/node/10777.

[271] Ibid., p. 67-68.

ISSN 2280-6164

linked to the US "probable cause" requirement,[272] as well as on the length of the various procedures.[273] However, for the purpose of electronic evidence, and apart from the fact that the major internet providers are located in the United States,[274] transatlantic cooperation on the collection of e-evidence remains problematic because no specific provisions, aimed at facilitating trans-border data exchanges, have been included.

For this reason, the Council has highlighted the need to foster discussions on possible ways to secure and collect e-evidence more effectively through the use of the already existing EU-US MLAT.[275] Furthermore, in light of the revelations of US mass surveillance activities by Edward Snowden, concerns about how European data are handled by American authorities in the context of intelligence and law enforcement activities have grown. In this context, EU-US Privacy Shield was formally adopted in July 2016 to protect data usage and provide clarity to businesses relying on data flowing from and to the two sides of the Atlantic.[276] The accord foresees safeguards and oversight mechanisms to limit data access by US authorities and affirms the absence of "indiscriminate or mass surveillance."[277] Nevertheless, the agreement is limited to the exchange of personal data for commercial purposes. The EU-US Privacy Shield will be complemented by the so-called EU-US "Umbrella Agreement," regulating the issue of transatlantic digital evidence exchange. Thus, they will set up a comprehensive data protection framework in cyberspace.[278] The agreement, signed in June 2016, is currently under discussion at the European Parliament, waiting for final approval.[279] It regulates the exchange of evidence for the purpose of prevention, investigation, detection and prosecution of criminal offences, including terrorism (art. 3), thus enhancing data protection rights in law

[272] The "probable cause" requirement "exist[s] where the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found". See Marie-Helen Maras, *Computer Forensics. Cybercriminals, Laws, and Evidence*, 2nd ed., Burlington, Jones & Bartlett Learning, 2015, p. 88. In some cases, it can be an obstacle if information to be provided are not sufficiently detailed. See Sergio Carrera et al., *Access to Electronic Data by Third-Country Law Enforcement Authorities*, cit., p. 68.

[273] Ibid.

[274] Anna-Maria Osula, *Accessing Extraterritorially Located Data: Options for States*, cit.

[275] Council of the European Union, *Review of the 2010 EU-US MLA Agreement*, Brussels, 7 April 2016, http://statewatch.org/news/2016/apr/eu-council-eu-usa-mutual-legal-assistance-review-07403-07-04-16.pdf.

[276] European Commission, *European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows*, Brussels, 12 July 2016, http://europa.eu/rapid/press-release_IP-16-2461_en.htm.

[277] European Commission, *EU-U.S. Privacy Shield, Factsheet*, July 2016, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.

[278] 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, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf.

[279] European Parliament, *Procedure 2016/0126(NLE): EU/USA Agreement: protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses*, http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2016/0126(NLE).

ISSN 2280-6164

enforcement cooperation. The Umbrella Agreement, once operational, will protect "all personal data" exchanged between police and criminal justice authorities of EU member states and US federal authorities (art. 3). However, it does not govern how law enforcement authorities may *collect* such data in the first place. Furthermore, it guarantees equal treatment for EU citizens, who will be able to enforce rights set down in the agreement (art. 19). Therefore, while enhancing cooperation in criminal matters, safeguards and guarantees have been be provided. For instance, provisions on clear limitations on data use and retention have been included. The development of new technologies and the increasing importance of cyberspace has brought vulnerabilities on different fronts.

Undoubtedly, the adoption of general requirements regulating the transfer of data represents an important step forward in terms of human rights protection; however, the problem of evidence-gathering in cyberspace should be addressed more directly. As mentioned, despite the proposed instrument, the EU has still not covered this issue with a common EU legislation. MLA procedures remain, however, not suitable for such a purpose and, consequently, inefficiencies in the fight against serious crime arise. Based on the principle of territoriality, in the case of collection of digital evidence, which are continuously flowing in cyberspace, MLA mechanisms should become more efficient to be effective in the digital era.

In such a scenario, enhancing the already existing MLA procedures, thus including, for instance, provisions to accelerate evidence-gathering in cyberspace, using as a model the already mentioned Budapest Convention, will not represent a solution, if the "territoriality principle" is not addressed. As emphasized by the Council, a closer cooperation with internet service providers should be further promoted.[280]

Furthermore, the European Union has generally adopted a "soft" EU integration on criminal matters, based on the "mutual recognition" principle, built upon minimum standards, rather than a complete harmonization, due, probably, to the high costs that harmonization would have raised in terms of political struggle. However, member states' procedures in the fight against crime differ consistently and given the cross-border dimension of those criminal activities, member states do not manage to effectively cooperate with each other, as the recent terrorist attacks in Europe have clearly shown. As a result, achieving criminal justice remains difficult if the EU fight against cross-border crime continues to lack a common ground of action.

While enhancing EU cooperation within the internal border, the EU cannot simply neglect its external dimension. Rather than supporting more "Europe-based cloud providers," as suggested by the EU Parliament,[281] a concrete framework to further

[280] Council of the European Union, *Council Conclusions on Improving Criminal Justice in Cyberspace*, cit.

[281] European Parliament, *US NSA: Stop Mass Surveillance Now or Face Consequences*, 12 March 2014, http://www.europarl.europa.eu/news/en/news-room/20140307IPR38203.

ISSN 2280-6164

facilitate law enforcement authority investigations, particularly in cross-border cases, when evidence is held by US communications providers, should be put forward. Following the European Security Agenda and the Council conclusions on improving criminal justice in cyberspace, the EU is currently discussing the possibility of implementing such a partnership. This framework should be built from a pan-EU harmonized instrument – possibly supplementing the EIO Directive – that enables direct contact between LEAs in one jurisdiction and service providers and data centers in another. The UK-US legislative agreement on cross-border data requests, if adopted, could represent a crucial precedent to enable efficient service provider cooperation with law enforcement.[282]

[282] The agreement, signed in July 2016 and currently waiting for the US Congress approval, would allow the British domestic security service to direct cooperate with US communication companies. See US Department of Justice, *Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data*, cit.

ISSN 2280-6164

5. Improving criminal justice in European Union cyberspace

by Tommaso De Zan

ISSN 2280-6164

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

After having assessed how the national authorities of three important member states collect e-evidence within and outside their jurisdictions, as well as the relevant EU regulations on judicial cooperation, this section aims to provide some practical suggestions on how to improve EU judicial collaboration in cyberspace. To do so, the first part analyzes the main trends that have emerged at the national level in order to learn whether the issues encountered can be generalized and solved with a common EU approach, the small sample of countries notwithstanding. In the second part, some key proposals on how to improve investigations in cyberspace are presented.

5.1 Analysis

The description of the procedures and challenges related to the collection of e-evidence within and outside the jurisdiction of the selected EU member states sheds light on some important commonalities and differences that need to be kept in mind. Four macro elements seem of major relevance: the impact on national legislation and investigative techniques of the recent terrorist attacks in Europe; although different in content and nature, similar legislative frameworks determining how e-evidence should be collected; the importance of judicial cooperation with the United States and US based service providers; the European Union as a common denominator and the related gaps concerning e-evidence in the Union's legislation.

The recent wave of terrorist attacks in Europe clearly had an impact in France, Germany and Italy. Although there is no fixed pattern in how the three countries have responded, Paris, Berlin and Rome have all resorted (or tried) to empower their national security and/or law enforcement authorities with new tools to effectively investigate serious crime and terrorism in cyberspace.

The terrorist attacks profoundly changed the security/legislative landscape in France, where, at the time of writing, the state of emergency is still in place. In particular, the new antiterrorism law foresees new simplified circumstances under which a computer seizure can occur, to the extent that the new powers granted to national authorities have prompted several observers to consider the balance between security and civil liberties "disrupted." Although mainly conceived to prevent terrorism, computer seizures are now permitted to target individuals who might represent a threat to national security. Generally, it appears that some of

the previous restrictions have been eased to facilitate national authorities' access to data stored in electronic devices. In Germany, a new version of *Bundestrojaner* was approved by the Ministry of the Interior in February 2016, whereas a new anti-terrorism bill was introduced in August 2016, expanding the competences of law enforcement and intelligence agencies. Moreover, the Ministry of the Interior is planning to establish a new agency whose main activity will be to decrypt communications. In Italy, encryption and Trojan horses animated parliamentary discussions and public policy debates on the possibility of exploiting these new instruments to prosecute criminals in cyberspace. Nonetheless, all these attempts have been warded off so far.

In sum, terrorism is one of the main drivers behind serious modifications to any law regulating investigations in cyberspace, giving the overall impression that, in the years to come, new policies that will include how e-evidence is collected might swing according to the perceived threat level.

The three countries have in place similar legislative frameworks determining how investigations in cyberspace are done. These are the privacy/data protection codes, national penal and criminal procedure codes, data retention policies and electronic communications codes.

All three countries have privacy/data protection codes to control and restrain how private data and other information are transferred to public or private organizations. France's level of data protection is considered high by most observers; in Germany too, privacy is protected by the Constitution and the Federal Data Protection Act; the Italian Privacy Code is an important piece of legislation and the President of the Italian Data Protection Authority often intervenes to assess the effects of new potentially harmful provisions on citizen's privacy.[283]

Regulations and procedures governing how e-evidence is collected and used in trial are elucidated in the various national penal and criminal procedure codes. Whereas the analysis of their principal common factors and differences is beyond the scope of the present endeavor, a few elements should be noted: all three countries seem to lack a proper definition of electronic evidence; while France and German laws detail the use of malwares in criminal investigations, Italian Code of Criminal Procedure does not, even though it is currently at the center of a contentious debate; some commonalities across the three legislations are found on procedures regarding the fight against cybercrime and references to the integrity and originality of data, these deriving from the implementation of the Budapest Convention.

All member states have in place data retention policies whose terms vary more or less greatly. In France, data retention is foreseen for a one year period. In Germany,

[283] National legislations regarding privacy will likely be modified once the new GDPR directive will be transposed into member states' jurisdiction by May 2018.

ISSN 2280-6164

a new data retention law coming into force in October 2015 constrains providers to retain traffic data for up to ten weeks. In Italy, a new law obliges providers to retain telephone and electronic communications traffic data until June 2017. All countries exclude content data from the requests they can advance to providers.

The most interesting finding from the analysis of the legislative scheme in place, however, derives from the presence of electronic communications codes at the national level that leave some uncertainties about who should be subject to it and whether they are being effectively enforced. Even though the French Code would compel national ISPs to retain data in order to cope with criminal investigations, French justice recently allowed national authorities to send formal requests to international ISPs as well. In Germany, national and international service providers must collaborate with LEAs, and if the provider refuses, it can be fined up to 100,000 euros, but it remains unclear whether this provision is effectively enforced. It is important to underline here that data retention policies are provisions within French and German Electronic Communications Code, so the uncertainty generated by the absence of clear definitions reverberates on data retention policies as well. In Italy, "operators" with an authorization to provide connectivity or electronic communications services are obliged, pursuant article 96 of the Electronic Communications Code, to cooperate with national law enforcement and provide "compulsory services," including interception of communications. Nonetheless, OTT/information society service providers are excluded, as at this time they do not have to seek an authorization to offer their services in Italy.

In terms of judicial cooperation with countries outside the EU, the relationship with the USA is of primary concern for all the three countries.

In an interesting and recent development, the French National Assembly voted two international conventions in January 2016 aimed at expanding criminal justice cooperation with the USA. The new conventions were devised to include the consequences of the use of digital technologies in criminal offenses and to facilitate French and American law enforcement agencies' access to information for criminal prosecution. According to the new framework, the information collected must be stored only for the time of the investigation and national authorities have to flag any mistake in data handling. Reportedly, the agreement took into account French wishes to protect data according to the level foreseen by French law. Finally, both parties can refuse to transmit information if this threatens national sovereignty and security.

Germany and Italy have not signed any new agreement with the USA and none will be signed in the near future. Both countries rely on MLATs they have signed (as in the case of Italy) or amended (Germany) in 2006 for the exchange of e-evidence between national authorities. Although actual statistics were not given, many interlocutors appeared disillusioned about the overall efficiency of the MLAT process concerning the acquisition of electronic evidence. Overall, procedures happen to be long because, on the European side of the Atlantic, it is not always easy for national authorities to write requests that can fulfil American legal standards

ISSN 2280-6164

of probable cause; on the American side, it seems American authorities are being inundated by requests asking their service providers to produce e-evidence, these being sent not only by France, Germany or Italy, but from countries all over the world. Furthermore, some sort of direct and voluntary cooperation between national authorities and a few American providers exists, but it seems mainly limited to the exchange of generic subscriber data. Both Berlin and Rome would like to see the institutionalization of a more constructive and efficient cooperation with service providers.

At the same time, judicial cooperation between the EU as a whole and the US should not and cannot be ignored, as data flow will only increase across the Atlantic for commercial and security purposes in the years to come. Recent revelations by American whistleblower Edward Snowden have inevitably rattled "digital relations" between the EU and the USA and have increased public awareness on how law enforcement and intelligence agencies should have access to data. In spite of what is already in place (the EU-USA MLA and the Budapest Convention) or what waits for the European Parliament's approval (the EU-USA Umbrella Agreement), better mechanisms between the EU and the US to advance cross border data requests seem inevitable.

As EU member states, France, Germany and Italy share important legislation that are vital for judicial cooperation on criminal matters. Mainly, this legislative framework is grounded in the parts of the Schengen agreement (1985), the Convention on Mutual Assistance in Criminal Matters between the member states of the European Union and its Protocols (2000) and the newly adopted European Investigation Order Directive (2014). Moreover, the Convention on Cybercrime (2001), which is not legislation of the European Union, but has been ratified by 25 out of 28 member states, adds another layer of commonalities.[284] The joint German-French declaration at the end of August 2016 offered other insights of possible ways to enhance judicial cooperation and, eventually, harmonization at the EU level. The Ministers of the Interior of the two countries, Bernard Cazeneuve and Thomas de Maizière manifested their intention to stave off obstacles hobbling state authorities' ability to counter the terrorist threat. Besides identifying solutions to pursue suspected terrorists communicating by means of encrypted services, the two ministers intimated the European Commission to propose new legislation that would compel communications and internet service providers to cooperate with the judicial authorities of the country where they offer their services (in what terms it was not specified).[285]

[284] Only Greece, Ireland and Sweeden have not ratified the Convention. For a full list see the Budapest Convention's website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

[285] "Par exemple, tous les opérateurs, qu'ils soient fournisseurs d'accès à Internet ou de communications électroniques, doivent être sujets aux mêmes obligations en ce qui concerne la coopération judiciaire dans les pays où ils assurent leurs prestations (indépendamment du pays où se situe leur siège juridique)." German Ministry of the Interior and French Ministry of the Interior, *Initiative franco-allemande sur les enjeux clés de la coopération européenne dans le domaine de la*

ISSN 2280-6164

ISSN 2280-6164

In spite of the limited number of selected countries, this analysis reveals that a great deal of common traits between them exist. From the source of enhanced investigative techniques, namely terrorism, and similar national legislative frameworks governing the collection of e-evidence to the importance of judicial cooperation with the USA and US based service providers, room for a common approach at the EU level exists. As presented in section 4, nonetheless, the EU normative framework is far from being definitive. Rules pertaining to the collection and exchange of e-evidence within the EU and between EU member states and foreign countries are still relying on rather cumbersome MLAT processes. In this respect, in all three countries, officials and experts agree on the necessity of stirring an EU level process to enable effective investigations in cyberspace. This might be preferable to member states' attempts to give their investigative powers extraterritorial effect, potentially putting overseas or multinational providers into difficult and incongruous jurisdictional situations . A harmonized, multinational accord on the scope of powers, and minimum protections, would ensure a clear, transparent and level playing field.

5.2 Policy suggestions

In this section, we seek to propose some suggestions to the issues delineated by the Council in its June 2016 conclusions and by the "Effective criminal justice in the digital age" document issued in November 2015.[286] In doing so, we expound a possible common framework that would tackle the majority of the issues underlined by the Council.

We will do it recalling the assumptions presented in the introduction and taking into account the analysis of the three case studies.[287] In recommending suggestions to improve criminal justice in cyberspace, we will also bear in mind: ongoing initiatives between countries and by non-EU institutions (CoE), the works of academics and civil society, but also policy statements from the major organizations representing service providers. The underlying assumption to include such a vast plethora of documents/positions is that a complex problem such as improving criminal justice in cyberspace cannot be tackled without a common effort entailing a multi-stakeholder approach. In doing so, we align ourselves with the same method followed by the European Commission, as presented in the first progress report of October 2016, being the Commission the

sécurité intérieure, cit.

[286] Council of the European Union, *Effective Criminal Justice in the Digital Age - What Are The Needs. State of Play* (14369/15), Brussels, 23 November 2015, http://data.consilium.europa.eu/doc/document/ST-14369-2015-INIT/en/pdf.

[287] Law enforcement should be able to effectively conduct investigations in cyberspace; International judicial cooperation should be consolidated to permit national authorities to obtain e-evidence when it is found or moves across jurisdictions; cyberspace should remain a safe environment where privacy is safeguarded.

main actor who will have to act and deliver solutions on the basis of the June 2016 Council's conclusions.[288] Before putting forward our recommendations, we dissect what should be the underlying principles that should engender what we believe is the set of legislation/policy changes most likely to have a significant improvement on criminal justice in cyberspace. We do so as we believe that once some principles are fixed, coherent and logical developments will follow accordingly. We expand our effort by seeking to give a coherent framework to "transatlantic" (EU-USA) judicial cooperation on cross-border data requests. This rests on the credence that, to fully address the Council's conclusions, only tackling the issue at the EU level would not make any significant change in the EU's attempt to improve criminal justice in cyberspace.[289]

1) Suggestion:

The subject-oriented approach should determine which national authority can be the "investigating state."
The national authorities of the country of habitual residence of the person whose data are sought have the authority to send the "production order" for the disclosure of data to the relevant service provider.
Service providers should abide by the law of the country sending the production order.

Rationale:

The issue of determining which national law the service provider should comply with when it receives data disclosure requests is becoming more and more central due to the digitization of criminal evidence and the structural characteristics of the internet. As Charlotte Conings argues, in a traditional object-oriented approach, where the evidence is to be found determines the location of the search, and thus the law enforcement authorities who should collect the sought evidence. Nevertheless, when it comes to electronic evidence, this notion has largely been surpassed, especially with the advent of cloud computing, where data can be stored anywhere and move across servers: "the internet reality separates the location of the data [...] from the location of the persons [...] in a way never before encountered."[290] In such a situation, it can become frustrating when the victim and

[288] European Commission, *First Progress Report towards an Effective and Genuine Security Union*, cit.

[289] The following recommendations do fully take into account the work of the "Cloud Evidence Group" of the Budapest Convention's Cybercrime Convention Committee and in particular the solutions presented in the latest report (*Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, cit.). However, we qualify our effort by circumscribing our suggestions to "transatlantic" (EU-USA) cross-border data requests, as the main scope of the paper is to feed insights into the ongoing policy-making process carried out by the EC to improve criminal justice in cyberspace.

[290] Charlotte Conings, "Locating Criminal Investigative Measures in a Virtual Environment: Where Do Searches Take Place in Cyberspace?", in *2011-2014 B-CCENTRE Legal Research Report*, p. 50, https://www.b-ccentre.be/wp-content/uploads/2014/06/B-CCENTRE-Research-Report-Legal_FINAL.pdf.

ISSN 2280-6164

the suspect are from the same country where the crime has been committed, but e-evidence is stored in another country. As Coning puts it: "the object oriented approach allocates the sovereign competence regarding the data to a state which shows very little connection with the investigated activity or person. In this way, the legal framework is completely alienated from the reality that it aims to regulate."[291] Paul De Hert and Gertjan Boulet note that "considering the lack of any effective international initiatives for trans-border investigations on the internet it would be unrealistic to prohibit national extraterritorial initiatives for trans-border access."[292] However, the dominant interpretation of international law asserts that gaining access to data that are not stored in the territory of the investigating state without the consent of the state where data are stored constitutes a breach of territorial sovereignty. To avoid conflict between countries, pinpointing whose national authority has the right to ask a service provider to disclose data is of paramount importance.

In our opinion, the subject approach should determine which national authority can be the "investigating state": (1) the country of the suspect's habitual residence; (2) the country of the victim's habitual residence; but in addition also (3) the country where the crime is being committed; (4) the country with well-founded links to the suspect or the victim. Nevertheless, the subject approach should be supplemented by the notion that it is the country of habitual residence of the person whose data are sought that has the authority to send to the relevant service provider the "production order" for the disclosure of data.

Switching from an object to a subject based approach sets a clear rule establishing which country should be the "investigating state," a change that is somehow inevitable if data move across servers around the world. An example might help to clarify: Italian law enforcement authorities are investigating a case of online child pornography and both the victim and the suspect reside in Italy. In this case, the investigating state coincides with the state who has the authority to send the production order. Hence, the Italian judicial authority has the right to ask the relevant service provider to produce the sought data. As an entity offering its services in the territory (see also policy suggestion 2), the service provider should comply with the production order sent by Italian authorities, regardless of where the data is located or where the legal headquarter of the service provider is. Notice here that there is already a tangible improvement from the current situation based on the object-oriented approach. In today's framework, if the national authorities investigating the crime are Italians, and the suspect or the victim reside in Italy, but data are stored in the USA or are found in cloud provider with legal headquarters in the USA, the service provider has to comply with US law. By adopting the subject

[291] Ibid., p. 60.

[292] Paul De Hert and Gertjan Boulet, "Cloud Computing and Trans-Border Law Enforcement Access to Private Sector Data. Challenges to Sovereignty, Privacy and Data Protection", in Future of Privacy Forum and Stanford Center for Internet & Society, *Big Data and Privacy. Making Ends Meet*, 10 September 2013, p. 23-24, https://fpf.org/big-data-privacy-workshop-paper-collection.

ISSN 2280-6164

approach, the law of the country where the data are stored or where the service provider's legal headquarters are located will not be the one determining if and how e-evidence is obtained.

Nevertheless, the subject approach should be supplemented by the notion that it is the country of habitual residence of the person whose data are sought that has the authority to send the "production order" for the disclosure of data. Adding this notion is an important guarantee to prevent foreign national authorities from accessing the data of a person who doesn't fall under their jurisdiction, the so-called "transborder data access." Again, an example might help to clarify: Italian law enforcement authorities are investigating a case of online child pornography. The victim resides in Italy, but the suspect resides in Germany. In this situation, Italian judicial authority should send a request of assistance to German authorities. After having evaluated the request, German authorities might decide to either cooperate or not. If they cooperate, they make a production order requesting the service provider to produce the sought e-evidence and then transmit it back to Italian judicial authorities. If German authorities do not cooperate, Italy will not be able to obtain the sought e-evidence. This applies to searches in real-time as well: it is the law enforcement of the country where the subject habitually resides that should perform the real-time search.[293] In this specific example, it is Germany that should perform the interception and not Italy. Nevertheless, the main guarantee of the principles proposed is also, potentially, its main setback. Going back to the example, if the Italian law enforcement authority is investigating a suspect who habitually resides in Germany, whether Italy is going to obtain the evidence of the suspect rests on the cooperation between Rome and Berlin. However, the issue here becomes the possibility of one country not cooperating with another, hence a problem of judicial cooperation between Berlin and Rome, rather than not knowing which state is the one investigating and which one has the authority to make the production order.[294]

These principles leave out the possible situation in which the country of habitual residence of the person whose data are sought is not known. In this extreme situation, when a "loss of location" situation derives, for instance, from the use

[293] Here an import specific scenario should be highlighted: when the subject moves to another state, does possibility to initiate or carry on the interception vanish? According to Conings, it is the country where the subject is located that should perform the search, rather than the one where it usually resides. For Conings, this seems reasonable also in terms of the principle of sovereignty: when the subject moves to another state, the possibility to continue the interception vanishes. (Charlotte Conings, "Locating Criminal Investigative Measures in a Virtual Environment", cit., p. 53.) However, according to the principle outlined in this report, it should be the country of habitual residence to perform the real-time search, when technically feasible. This is probably the best solution, as the interception should not be performed by a country with little stakes in the process. Nevertheless, to avoid creating conflict between countries, the country of habitual residence might notify the country where the interception takes place.

[294] The proposed approach is different from Coning's as the author does not seem to distinguish between the possibility of having an "investigating state" and one with the legal authority to send service providers a production order.

ISSN 2280-6164

of anonimising tools, although international cooperation should be preferred, if one follows the subsidiarity principle, whereby the least drastic solution has preference, "if direct access [...] is the only way to attain a satisfactory result, the investigating state shall feel compelled to use that competence if the conditions in accordance with the national law are satisfied."[295] Once country of habitual residence is ascertained, and if this does not coincide with the investigating state, the latter should then send a request for assistance to the authorities of the country of habitual residence.

This mechanism puts into a coherent system a set of rules that in other circumstances have been regarded as plausible:

> In this regard the location of habitual residence of the investigated person, and the nationality of the victim or of the suspect would follow as a logical ground for jurisdiction. With regard to cooperation with private sector, the connection of the service provider to the territory of the investigating state was put forward, referred to as a "business link". According to this approach, any service provider that provides services in the territory of a given state is considered to be bound by that state's legal framework and should therefore cooperate with law enforcement on the basis of domestic orders.[296]

It is important to make an important distinction here. Service providers are not complying because they are merely offering their services in a country. They are complying because the country which can legally send a production order has asked them to do so. By assuming this principle, the reverse indeed would not be possible. If a service provider were legally bound to comply with a production order merely because it is offering its services in a country, that would be deleterious, as it would allow foreign countries to access data of citizens that are not their habitual residents. And this is something that, also in the name of security, should not be pursued, unless judicial cooperation between countries is established. Nonetheless, to make this mechanism effective, changes to European and American legislations should be brought about.

2) Suggestion:

A new common European framework should give a common definition of what constitutes:
a) E-evidence
b) Service provider
c) Offering services in the EU.

[295] Charlotte Conings, "Locating Criminal Investigative Measures in a Virtual Environment", cit., p. 69.

[296] Netherlands EU Presidency 2016, *Crossing Borders: Jurisdiction in Cyberspace. Conference Report*, 23 March 2016, p. 5, http://data.consilium.europa.eu/doc/document/ST-7323-2016-INIT/en/pdf. See also the conference page: https://english.eu2016.nl/events/2016/03/07/crossing-borders-jurisdiction-in-cyberspace.

ISSN 2280-6164

ISSN 2280-6164

Rationale:

So far, wanting definitions have generated a remarkable conundrum. On the one hand, service providers *de facto* offering their services in Europe, argue that, if they comply with the law of one member state, they might be breaking the law in the country where their legal headquarters are located or the country where the data are stored. The case of the Microsoft executive who was charged in Brazil for not handing over records of a Brazilian's Skype calls that were stored in the USA, as doing so would have been a felony in the USA, is indicative of the traps of the current international framework in place.[297] On the other hand, it seems plausible that national authorities are seeking a direct contact with service providers not necessarily (or not only) because they do not want to undergo the MLAT process, but because they (or related national laws) do not make a distinction between the various "types" of service providers and believe that, as *de facto* offering services on their territory, service providers should comply with their legislation. Adopting new and clear-cut definitions can be beneficial for both national authorities and providers: it would meet the expectations of those member states, like France and Germany, which would like to see advanced a new legislation regulating cooperation between national authorities and service providers operating in Europe; but it would also be beneficial to service providers offering their services in the EU to dispel much of the doubts about the current conflicting frameworks they have to comply with. Henceforth, the following suggestions should be followed:

First, a common definition of e-evidence across Europe would enhance the understanding of what should be collected, exchanged and preserved and obviate the dearth of a proper definition within member states' national criminal law procedures.

Second, after a careful review of the case studies, it seems that tensions between some EU member states' national authorities and service providers also stem from uncertainties related to who should be subject to their respective national electronic communications codes. At the moment, it is unclear whether the so-called OTT or Information society service providers have or should comply with the same rules of telecommunications/electronic communications providers. A similar conclusion can be inferred from a recent Council document published by Statewatch, which reports the answers of member states' law enforcement authorities on the specific topic of encryption:

> service providers are obliged according to national law to provide law enforcement authorities with encryption keys/passwords; a judicial order is not always required. However, in general, the answers do not make a distinction whether this obligation applies only to the providers of electronic communications services or also encompasses the providers of

[297] Dina Bass, "The Case That Has Microsoft, Apple and Amazon Agreeing for Once", cit.

information society services.[298]

A new common European framework should therefore adopt a definition of "service provider" encompassing all service providers offering communication services, including information society/OTT service providers.

Third, a common definition should define what it means to be "offering a service in the territory." The same is reported by the CoE: "Clarification is needed as to when a service provider is indeed present or 'offering a service in the territory' of a state and is thus subject to a domestic production or other type of coercive order."[299] Clarifying whether a service provider is offering its services in the EU or not it is of primary importance, not to determine which country should be sending the production order, but to bind the service provider to accept it when it receives one. Regardless of the presence of the provider's headquarters or another legal entity on the territory of a member state, if the service of a provider is authorized to offer its services (meaning that an EU user can subscribe and access them), the service provider should be considered to be offering its services in the member state.

3) Suggestion:

A new common framework should make clear the application of the principle of mutual recognition enshrined in the EIO to e-evidence.

Rationale:

If it is true that the new EIO Directive introduces an automatic mutual recognition of investigation orders that allows "a judicial decision, which has been issued or validated by a judicial authority of a member state, to have one or more specific investigative measure(s) carried out in another member state to obtain evidence in accordance with the directive,"[300] it would specifically tackle the example we have outlined in suggestion 1. Going back to it, in a situation in which the victim resides in Italy but the suspect is German, Italy would have to send an EIO to

[298] Council of the European Union, *Encryption of Data: Mapping of the Problem. Orientation Debate*, Brussels, 21 October 2016, p. 4, http://www.statewatch.org/news/2016/oct/eu-encryption-orientation-debate-13434-16.pdf. The document however also stressed that: "Secure processing is an important element of personal data protection, and encryption is recognised as one of the security measures in the recently adopted General Data Protection Regulation. Companies, public administrations and individuals are encouraged to use encryption to protect their data and electronic communication. The e-Privacy Directive also encourages the use of encryption technologies to protect users' communications. However, the opportunities offered by the encryption technologies are also exploited by criminals in order to hide their data and potential evidence, protect their communications and mystify their financial transactions." Ibid., p. 2.

[299] T-CY Cloud Evidence Group, *Criminal Justice Access to Electronic Evidence in the Cloud: Informal Summary of Issues and Options under Consideration by the Cloud Evidence Group*, 17 February 2016, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8.

[300] Council of the European Union, *Council Adopts the "European Investigation Order" Directive* (7559/14), Brussels, 14 March 2014, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/141495.pdf.

ISSN 2280-6164

German authorities to obtain the sought e-evidence. This is entirely coherent with the principles outlined in suggestion 1. Notice also that, as we have seen in Section 4, the directive has listed grounds for refusal which include "national security interests," in addition to traditional restrictions such as immunity or privilege and incompatibility with the executing State's obligations. As we have noticed before, if a country refuses to hand over the sought evidence, it is an issue of judicial cooperation rather than an issue of jurisdiction. If the goals of the Directive are met ("make judicial cooperation on investigations faster and more efficient," "limit the grounds for refusal by another EU state to execute the order," "sets deadlines for carrying out the investigative measures and requires that the recognition or execution should be carried out with the same priority and speed as for a similar domestic case"),[301] it would significantly improve judicial cooperation on e-evidence exchange, which now still rests on rather long and cumbersome MLAT processes. The new directive will have to be transposed into member states' legislation by May 2017. At the moment, however, it is unclear whether e-evidence is being included as a type of evidence that can be sought with an EIO. Hence, the new common framework, or an amendment to the EIO Directive, should make clear the application of the EIO to electronic evidence.

4) Suggestion:

The EU should seek an agreement on cross border data requests with the USA.

Rationale:

The proposed common European framework would necessarily entail a new form of judicial cooperation with third countries whose legislation influences the operations of the main international service providers. In the digital domain, the relevance of the United States urges the EU to establish a new relation with Washington. The new accord might take multiple forms, including new amendments to the EU-USA MLA, changes to the EU-US Umbrella Agreement, or a new bilateral agreement. As an alternative – if unity across the EU is not achievable – member states should pursue renewed bilateral treaties, or "opt-in" multilateral options such as a new and expanded Protocol to the Budapest Convention.

A new common framework that compels American providers to deliver data to EU law enforcement agencies would prove ineffective, or even useless, if relevant American legislation is not modified in order to make it legal for US service providers to hand over data to EU national authorities. In particular, a new agreement should prompt changes to ECPA that allows service providers to hand over subscriber and traffic data on a voluntary basis, but does not compel them. Based on the principles outlined in suggestion 1, a new agreement with the EU might indeed permit US based service providers to deliver generic subscriber, traffic and content data to EU national authorities that lawfully send a "production order" to a service provider. It should be underlined that a new agreement would make the reverse valid too:

[301] Ibid.

ISSN 2280-6164

in the context of criminal investigations and when precise legal safeguards are met, EU providers "offering their services in the USA" would need to disclose data to US authorities, if they receive a valid production order. In fact, one should not believe the myth that difficult relations have been beleaguering only relations between American providers and European national authorities. As the CoE put it: "European providers normally choose not to disclose any data directly to criminal justice authorities in foreign jurisdictions, not even in emergency situations."[302] An agreement of this sort would then significantly improve judicial cooperation on both sides of the Atlantic.

Solutions in line with these proposals are emerging in the USA as well, and the possibility of adopting such reforms have spurred recent legislative initiatives within the US Congress. In May 2016, Sen. Orrin Hatch introduced in the Senate the International Communications Privacy Act (ICPA), whereby a governmental entity might require, only pursuant to a warrant, the disclosure of content data by a provider of electronic communication service or remote computing service regardless of where the content might be. The warrant can call for the content's disclosure of the subscriber or customer that is:

> (i) a United States person; (ii) physically located within the United States; (iii) a national of or located in a foreign country or countries where any of those countries has an applicable Law Enforcement Cooperation Agreement with the United States [...] and the Central Authority for each such country with such a Law Enforcement Cooperation Agreement provides written certification that the disclosure may be had or does not object to the disclosure within 60 days after formal submission of a request for such certification; or (iv) a national of and located in a foreign country or countries where none of those countries have an applicable Law Enforcement Cooperation Agreement with the United States.[303]

This proposal is consistent with the principles presented in suggestion 1. The USA would be able to obtain data of Americans and foreign nationals regardless of where they are stored, inasmuch as a warrant has been obtained by the prosecuting authority and if the country of the citizen/resident does not object to the disclosure. A "transatlantic solution" of this kind does not seem so quixotic if one observes what it has been agreed or signed lately between the USA and other, although exiting, EU member states. After long negotiations, an agreement on cross-border data

[302] T-CY Cloud Evidence Group, *Criminal Justice Access to Electronic Evidence in the Cloud: Informal Summary of Issues and Options under Consideration by the Cloud Evidence Group*, cit., p. 3.

[303] US Congress, H.R. 5323: *International Communications Privacy Act*, 25 May 2016, https://www.govtrack.us/congress/bills/114/hr5323/text/ih. Numerous "tech groups," including the Consumer Technology Association, the Internet Association, CompTIA, and ACT the App Association have urged Congress to pass the bill, which would settle "any confusion over the legal data protections available to foreigners." See Amir Nasr, "Tech Groups: Pass International Communications Privacy Bill", in *Morning Consult*, 14 July 2016, https://morningconsult.com/?p=39006.

© 2016 IAI
ISSN 2280-6164
DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

requests between the United Kingdom and the US was signed in July 2016.[304] The legislative measure, which is currently waiting for US Congress approval, would allow British domestic security services to directly contact US communications companies in order to obtain electronic evidence in the context of criminal investigations. While excluding intelligence gathering activities, the law applies specifically to support law enforcement and covers both content and traffic data, as well as interception and access to stored data.[305] According to the draft legislation, both access and veto rights apply reciprocally, meaning that both governments have to remove potential obstacles to let the direct access to the providers take place, and both have the right to block the access to data if the request does not fulfil the necessary requirements. Clearly, if the US Congress approves the agreement, it will represent a first important step forward for the future development of EU-US cooperation with US communications service providers.[306] Whereas it is true that, as experts have noticed in the various interviews, such an agreement was made possible because the two countries share the same common law system, some bold reformers are pushing for legislative change to permit service providers to have direct contacts with non-US national authorities. Orin Kerr has proposed changes to ECPA that would allow American service providers to lawfully respond to valid requests from non-US countries to deliver e-evidence about non-US citizens outside of the United States, if strict legal safeguards and human rights protection are in place.[307] In spite of being fraught with difficulties, which could be worked out during an exacting proposal phase, a solution of this kind might be facilitated if on the other side of the negotiating table there is the EU, where protection of privacy and human rights are generally considered to be high.

Although the overall process would be significantly streamlined by adopting the principles of suggestion 1, MLAT requests will not disappear. In a hypothetical scenario in which an EU member state seeks data of a US habitual resident, the EU member state would have to ask US authorities to make a production order and then transmit the data. Although quite futuristic, as Sergio Carrera has already argued, the ideal solution would be "the adoption of a Transatlantic Investigation Order (TIO) system" with the primary aim "to speed up and make more efficient cooperation between US and EU authorities in the field of criminal justice."[308]

Finally, in the wake of a new EU data retention policy (see suggestion 6), the agreement should also aim to establish a data retention policy in the US and make those two policies aligned in order to make electronic evidence available for

[304] US Department of Justice, *Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data*, cit.

[305] David Kris, "U.S. Government Presents Draft Legislation for Cross-Border Data Requests", cit.

[306] Ibid.

[307] Orin S. Kerr, "The Next Generation Communications Privacy Act", in *University of Pennsylvania Law Review*, Vol. 162, No. 2 (2014), p. 373-419, http://scholarship.law.upenn.edu/penn_law_review/vol162/iss2/3.

[308] Sergio Carrera et al., *Access to Electronic Data by Third-Country Law Enforcement Authorities*, cit., p. 80.

ISSN 2280-6164

criminal investigations on both sides of the Atlantic.

5) Suggestion:

The common framework should establish specific mechanisms determining how service providers handle production orders and produce e-evidence.

Rationale:

Standardized mechanisms and procedures, developed in close collaboration with service providers, should be devised on how they will handle formal requests, so as to avoid their having to develop autonomous (and maybe precarious) methods of data handling.

Direct cooperation between law enforcement agencies and service providers would need to ensure that electronic evidence is produced without altering its originality and integrity and can be securely transferred.

According to the mechanism of suggestion 1, it is reasonable to believe that service providers will have more production orders to satisfy in the future. In this sense, some further suggestions might be taken into consideration to improve the overall process of data requests: (1) service providers might establish a new section of their websites (or a dedicated online platform) where member states' national authorities can request and obtain the sought electronic evidence; (2) a unique format of data request should be advanced; (3) prioritization according to the type of data requested: the more "important" the content requested (content data should be ranked at the highest level), the higher the priority of the request to be processed; (4) adequate staffing within the service providers' legal departments.[309]

An "emergency data request form" should be established to allow a quicker disclosure of data in the wake of possible terrorist attacks, kidnappings or life-threatening situations. Similarly to what is already foreseen by the Budapest Convention, a 24/7 point of contact within the service provider's legal department should be established to deal with such emergency requests.

Although service providers should not be put in the position of evaluating the legality of the production order, which derives from the authorization of the judge from the country which has the authority to send it, internal mechanisms that further scrutinize received production orders should be put in place. In case of a dispute with a country's national authorities, the service provider might send the production order to a newly established third-party agency in charge of evaluating controversial requests.

[309] Options 1, 2, 4 are presented in Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, Washington, Global Network Initiative, January 2015, https://globalnetworkinitiative.org/node/367. For more options on how to improve the MLA process, see Cybercrime Convention Committee, *T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime*, cit.

ISSN 2280-6164

The new EU common framework should prompt changes in member states' criminal procedure laws to allow e-evidence obtained directly from service providers to be available in criminal proceedings.

6) Suggestion:

A new common framework should foresee a new EU data retention regime.

Rationale:

According to Eurojust, the subsequent fragmentation of the EU legal framework on data retention following the invalidation of the 2006 Data Retention Directive by the EU Court of Justice, may negatively influence the effectiveness of criminal prosecutions at the national level, but also on cross-border judicial cooperation within the EU and with third countries. As the report put it, some member states lamented the fact that "it is problematic and challenging that national data retention legislations among close cooperation partners differ significantly," as there is no legal common basis to proceed with the request of data retention from one state to another, if not in the form of an MLA request.[310] The European Commission should recognize the demand amongst member states and review periodically its official position not to pursue a new legislation. Clearly, any measures requiring retention must respect fundamental rights and the principle of proportionality that, according to the CJEU judgment, the 2006 Directive exceeded. Helpfully, subsequent CJEU case law has provided further guidance in that respect.

7) Suggestion:

The common framework should enhance the role of Eurojust.

Rationale:

Eurojust, and in particular the European Judicial Cybercrime Network, should become the hub for specialized judicial expertise in cyberspace investigations, facilitating member states' cooperation and exchange of expertise/information in relation to criminal procedure law and e-evidence collection.[311]

Although sovereignty will remain with member states, the agency might also propose further harmonization and provide specific recommendations on procedural legal requirements that should regulate the specifics of national authorities' production orders to be sent to service providers. With the mechanism proposed in suggestion 1, the service provider will have to comply with the law of the country sending the production order. Thus, it is the country sending the

[310] Council of the European Union, *Eurojust's Analysis of EU Member States' Legal Framework and Current Challenges on Data Retention*, Brussels, 26 October 2015, p. 11, http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf.

[311] Council of the European Union, *Council Conclusions on the European Judicial Cybercrime Network*, cit.

ISSN 2280-6164

production order that will determine the "lawfulness" of the production order. In this sense, there will not be any "probable cause" legal requirement to meet, as requests for data access will not be examined by US authorities anymore , as it often happens nowadays. However, in our opinion, "direct relations" with service providers should not lead to indiscriminate access to users' data. In general, a production order should be sent when, in the context of crime prosecution and under the specific conditions regulated by member states' criminal procedure laws, the judicial authority of a country authorizes it. In this regard, it is possible to envisage that different legal requirements should govern what kind of data can be sought. Eurojust might suggest what legal requirement should be met to request generic subscriber data, traffic data and content data.[312] To the extent safeguards are established, these might be harmonized at the European level to ensure that users understand the level of protection in the Union and can expect consistent treatment of their data according to common norms. This could be established in a systematic fashion, for example, by an official "whitelisting" procedure, similar to the one which the European Commission has administered for over two decades under the Data Protection Directive (95/46/EC), which generally prohibits transfers of personal data to countries that do not offer "adequate" standards of data protection.[313] Practically, Eurojust might suggest what legal requirement should be met to ask generic subscriber data, traffic data content data.[314] Statistically, the CoE reports that parties to the Budapest Convention mostly request generic subscriber data, followed by traffic data and finally content data.[315] Although this result might have been influenced not by the actual investigation needs but by the difficulties of obtaining traffic and content data in the current framework, if the statistics point to the right cause. One could imagine that assigning different "standards of proofs" according to the type of data sought might significantly streamline the entire process. To obtain generic subscriber data, the judicial authority might require a "limited level of suspicion," for traffic data a "medium level of suspicion," for content data a "high level of suspicion." This would be in line with what the Council said ("less rigorous legal processes could be envisaged for [...] specific categories of data")[316] and the general sentiment that certain data (certainly generic subscriber data, it is not clear for traffic data) "represents a lesser interference with the rights of individuals."[317]

Eurojust might also suggest proper legal standards governing the use of highly contentious investigative tools and techniques, especially in the context of the EU's common fight against serious crimes and terrorism, which has been the primary

[312] Interview, Brussels, October 2016.

[313] Directive 95/46/EC of 24 October 1995, Article 25(1).

[314] Ibid.

[315] Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, cit.

[316] Council of the European Union, *Council Conclusions on Improving Criminal Justice in Cyberspace*, cit., p. 3.

[317] Cybercrime Convention Committee, *Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, cit., p. 52.

ISSN 2280-6164

reason prompting EU member states to employ more powerful investigative tools, as we have seen from the analysis of the case studies.

8) Suggestion:

The new EU common framework should enhance the role of Europol.

Rationale:

Europol might constitute the EU knowledge hub for the dissemination of best practices in the field of digital forensics, including the possibility of setting common standards in the use of highly contentious investigative tools and techniques, especially in the context of the EU common fight against serious crimes and terrorism.

Europol should expand its activities to include supporting EU member states in cyberspace investigations. While hard to imagine now, Europol might also assume a more direct role in investigations, especially when a number of systems are used simultaneously and when electronic evidence shifts from one jurisdiction to another within the EU.

ISSN 2280-6164

Conclusions

The main goal of this report was to feed some policy suggestions into the ongoing debate that is animating EU institutions on possible solutions to improve European criminal justice in cyberspace. There are a few takeaways from this endeavor. The subject-oriented approach should determine which country can be the "investigating state;" nevertheless, it is the country of habitual residence of the person whose data are sought that should have the authority to send a "production order" for the disclosure of data to the relevant service provider. Since it is offering its services there, the receiving service provider should then abide by the law of the country sending the production order. To make this work, a series of inevitable actions should follow. The EU should adopt a common framework clearly defining "e-evidence," what is a "service provider" and what it means to be "offering its services in the EU." To make judicial cooperation more efficient, the EU should make clear the application of the principle of mutual recognition enshrined in the EIO to e-evidence. Yet, all these much needed reforms would be of little help, if legislation change is not pursued in relevant third countries. Having ascertained the predominant role of the USA and of US based service providers, the EU should sign a cross-border data request agreement with the US Government. The agreement should make sure that relevant American legislation, namely ECPA, is changed to allow US service providers to disclose data to EU authorities, when these can legally send a production order. The reverse should be made possible too. Such an agreement is feasible given EU high standards in data protection and human rights, and would probably be welcomed in the USA as well, where policymakers are advancing solutions (such as ICPA) going in the same direction. The transatlantic framework would be reinforced and the lingering paradox of imposing US criminal law upon EU criminal cases will be dispelled. The report puts forward a series of other policy suggestions, including a common EU-USA data retention regime, an enhanced role for Europol and Eurojust and the establishment of specific mechanisms regulating how service providers should handle production orders.

The proposed recommendations are certainly daring but are much in need. At a time when the terrorist and other threats are at their highest in the history of the EU, law enforcement agencies must be given the right technological tools and legal instruments to effectively pursue criminals and terrorists who employ ICT and cyberspace to commit their crimes.[318] The extant desynchronized international framework is not suitable for the task. The mechanism based on territoriality and the MLA is slow and ineffective, especially when data move across jurisdictions, or criminals and terrorists hide their locations with anonimising tools. National

[318] Barbara Starr, "Terror Threat in Europe 'as High as It's Ever Been,' Officials Say", in *CNN*, 3 February 2016, http://cnn.it/20qXQLz.

ISSN 2280-6164

authorities are thus turning to service providers to receive more collaboration in their effort to keep citizens safe. While being willing to cooperate, service providers are often nonplussed when they are caught between the fires of different jurisdictions, as cooperation with a national authority in one country might produce a felony in another. Faced with this jumble, countries' parliaments and courts are trying to tackle these issues autonomously. While being perfectly lawful, these attempts rest on the false assumption that one single actor, although cohesive, might solve a set of strictly correlated problems that would require the effort of several stakeholders to achieve a solution. Indeed, a new courageous international framework is possible, and is the best guarantee for the online privacy of users.

The proposed policy suggestions do not offer all answers, but might be a good place to start. If adopted, and in the context of crime investigation, they will not require any forced data localization policy in Europe or elsewhere by states eager to control access to citizens' data; it will not make it necessary to resort to international hacking, if not in extreme cases and until the residence of the person whose data are sought is known; it will make decryption tools useless, as data will be made available by direct contact with service providers, when legal requirements are met; it will provide much clarity for service providers, which will not have to choose between the lesser of two evils when confronting different jurisdictional claims; citizens' privacy will be upheld.

Once clear guidelines are established, every single actor in the game must do his part and play according to the same rules. Trust between law enforcement agencies, judicial authorities, users, civil society advocates, service providers, EU and USA institutions should permeate the process. Stakeholders should recognize that this kind of trust is hard to build but easy to elapse, and continuous revelations about opaque programmes do not necessarily inspire such a sentiment.[319] Snubbing the various stakeholders' needs will only exacerbate conflict and, instead of antagonizing imaginary "privacy vs security" groups, all actors should commit themselves to clear frameworks and work together to ensure their application.

Updated 21 November 2016

[319] Joseph Menn, "Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence – Sources", in *Reuters*, 4 October 2016, http://reut.rs/2dGeeRM; Joseph Menn, Dustin Volz and Mark Hosenball, "Yahoo Scanning Order Unlikely to Be Made Public: Source", in *Reuters*, 25 October 2016, http://reut.rs/2eIh7DJ.

ISSN 2280-6164

List of acronyms

BKA	Bundeskriminalamt (Federal Criminal Police Office)
CCC	Chaos Computer Club
CJEU	Court of Justice of the European Union
CNIL	Commission Nationale de l'Informatique et des Libertés
CoE	Council of Europe
CPP	Codice di procedura penale (Italian Code of Criminal Procedure)
DPA	Data Protection Authority
EAW	European Arrest Warrant
ECHR	Council of Europe Human Rights Convention
ECMACM	European Convention on Mutual Assistance in Criminal Matters
ECPA	Electronic Communications Privacy Act
EEW	European Evidence Warrant
EIO	European Investigation Order
FBI	Federal Bureau of Investigation
GDPR	General Data Protection Regulation
GG	Grundgesetz (Basic Law for the Federal Republic of Germany)
ICPA	International Communications Privacy Act
ICT	Information Communication Technologies
IRG	Gesetz über die internationale Rechtshilfe in Strafsachen (Act on International Cooperation in Criminal Matters)
ISIS	Islamic State of Iraq and Greater Syria
ISP	Internet Service Provider
LEA	Law Enforcement Agency
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
NSA	National Security Agency
OTT	Over-the-top content
RCIS	Remote Communication Interception Software
RiVASt	Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (Guidelines on Relations with Foreign Countries in Criminal Law Matters)
SIS	Schengen Information System
SOC	Serious and Organized Crime
StGB	Strafgesetzbuch (German Criminal Code)
StPO	Strafprozessordnung (German Code of Criminal Procedure)
TIO	Transatlantic Investigation Order
TKG	Telekommunikationsgesetz (Telecommunications Act)
TKÜ	Telekommunikationsüberwachung
TKÜV	Telekommunikations-Überwachungsverordnung (Telecommunications Interception Ordinance)
Zitis	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Central Office for Information in Security Sphere)

ISSN 2280-6164

ISSN 2280-6164

DOCUMENTI IAI 16 | 17 - NOVEMBER 2016

Istituto Affari Internazionali (IAI)

Founded by Altiero Spinelli in 1965, does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. The IAI publishes an English-language quarterly (The International Spectator), an online webzine (AffarInternazionali), two series of research papers (Quaderni IAI and IAI Research Papers) and other papers' series related to IAI research projects.

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest DOCUMENTI IAI

16 | 17	Tommaso De Zan and Simona Autolitano (eds.), *EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace*
16 | 16	Bianca Benvenuti, *The EU-Turkey Deal and Its Implications for the Asylum Capacities of EU Border Countries*
16 | 15	Matteo Brunelli, *European Security Governance and Transatlantic Relations*
16 | 14E	Francesca Bitondo and Paola Sartori, *NATO Defence Planning After the Warsaw Summit*
16 | 14	Francesca Bitondo e Paola Sartori, *La pianificazione della difesa della Nato dopo il vertice di Varsavia*
16 | 13	Alessandra Scalia e Nicolò Sartori, *Il futuro dei lanciatori europei: opportunità e sfide per l'Italia*
16 | 12	Sabrina Palanza, *Internet of things, big data e privacy: la triade del futuro*
16 | 11	Andrea Dessì, *Re-Ordering the Middle East? Peoples, Borders and States in Flux*
16 | 10	Roberto Aliboni, *La politica libica dell'Italia*
16 | 09	Ettore Greco, *L'eredità del passato, le sfide del futuro. L'Istituto Affari Internazionali e il "metodo" Spinelli*