RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN: 2704-7318
Fascicolo 2-2019
DOI: 10.32091/RIID0011

Modern Issues in Cyber Forensics and Digital Intelligence: A Critical, Case-Studies-Based Overview in Light of the Announced Legislative Reforms

Stefano Fantin • Giuseppe Specchio • Peggy Valcke

While both international and European law-makers are currently in the process of introducing new laws regulating the fight against cybercrime and the exchange of digital evidence amongst competent authorities, this paper elaborates on a series of investigative challenges deriving from the application of current cybercrime norms in a number of jurisdictions, unveiling a tension between the current legal system and its interpretation by the law enforcement and judicial community. This study analyzes the research undertaken on the legal and regulatory uncertainties observed in the Italian framework, as well as in other European and non-European jurisdictions, by ways of comparative analysis. The main international legal instrument on cybercrime is the Council of Europe's Convention on Cybercrime ('Cybercrime Convention'), signed in 2001 and then ratified by almost 60 countries worldwide over the last 17 years. Aimed at raising awareness to national and international policy and law makers, this paper intends to critically demonstrate how the implementation of such a treaty into domestic laws has not always been smooth. It often presents interpretative issues, which add up to the growing difficulties for both law enforcement and judicial bodies to cope with the challenges arising by countering new and innovative forms of criminal activities in the cyberspace.

Cybercrime – Digital Forensics – e-Evidence – Cybercrime Convention

1. Introduction

There is nothing novel when saying that the role of cybercrime is enormously increasing in law enforcement and security strategies. Broadly speaking, this is certainly an effect of the digitalization of our lives. According to the Internet World Stats[1], users in 2001 were 458 million against the 4157 millions of today. The new digital revolution[2] brings along astounding figures and new phenomena. With the advent of IoTs, our society is seeing the birth of an internet with three dimensions, and who knows what new scenarios are yet to come.

Regulating the internet has proven to be quite a difficult task. Even more so for harmonizing and enforcing criminal laws that, until a while ago, solely

The research for this article has been performed and partially funded by the projects CIF (Cybersecurity Initiative for Flanders) and DANTE (European Commission, GA 807440).

S. Fantin, LL.M., is a Doctoral Researcher at the Center for IT and IP Law at the KU Leuven University, Belgium. G. Specchio, PhD, is a Lieutenant at the Reparto Operativo Speciale, Arma dei Carabinieri, Italy. P. Valcke, PhD, is Professor of Law at the Center for IT and IP Law at the KU Leuven University, Belgium and Visiting Professor at Bocconi University in Milan, Italy.

pertained to offline interactions. Likewise, criminals found fertile ground in the cyberspace, rapidly adapting their business model to new digital opportunities. Methods to conceptualize cybercrimes are now greatly differentiated. The traditional silo-based approach, which considered cybercrime as a standalone cluster of online felonies, has rapidly been replaced by a two-fold one, which embraces crimes enabled or facilitated by the internet as an extension of offline conducts[3].

In many countries, the most influential piece of domestic legislation on cybercrime is the implementation into national law of the Cybercrime Convention[4] by the Council of Europe (CoE). Drafted almost twenty years ago (2001), today counts almost 60 countries between signatories[5]. It is admittedly the most important legislation in the field.

Almost two decades later, the CoE has started the process of amending the Convention[6], with the great pleasure of many cybercrime experts and scholars who have been voicing for a prompt reform over the recent decade[7]. With the addition of a new Protocol, *inter alia* on enforcement cooperation and electronic evidence, the legislator in Strasbourg is trying to learn from the past while inevitably looking at what is awaiting us over the next years. Alongside the efforts of the CoE, also the European Union is currently undertaking legislative steps in order to harmonize rules on the exchange of electronic evidence across the Union and beyond its territories[8]. The moment is crucial, therefore, as the new rules will likely influence the ways investigation and prosecution will be undertaken in the future.

The goal of this article is two-fold: first, it intends to shed light on how the fight against cybercrime over the past decades was significantly shaped by technological advancements, new models in criminal activities and, most importantly, difficulties in the implementation and in the interpretation of existing rules. Secondly, based on the elements analyzed, it aims to identify a set of gaps between the law as it stands and its enforcement.

The article therefore primarily targets the community of legislators at various levels – including the CoE, the European Union and its Member States – involved in the reform of the current legal frameworks on cybercrime investigations. Moreover, it will also be of relevance for those professionals enforcing the law, particularly public officials tasked with cyber forensics in the course of a criminal investigation.

Based on the findings arising from the case studies presented below, this article argues that current efforts in reforming the cybercrime legal landscape should take into account two key takeaways. First, a mutual understanding between different levels (CoE, European Union and domestic laws) on the legal and interpretative challenges in the respective framework is needed. Second, effective cybercrime norms call for a deep reflection on their human rights implications, especially in regard to the right to privacy and data protection.

1.1. Methodology

The analysis that underpins this article is carried out through doctrinal research based on the traditional legal sources, i.e., legislation, case law and scholarly literature. The Italian situation is used as a case study throughout the text and, where relevant, enriched with functional comparative elements drawn from other jurisdictions, including the UK and Belgium[9] (in light of the background and linguistic skills of the authors).

The case studies below will outline and inform how cyber investigators in Italy and beyond have to operate in a context of legal uncertainty because of obsolete or unclear legal rules. Particular attention will be paid to challenges in defining prosecutorial competence, seizure and acquisition of electronic data, retention and expert examinations. Depending on the issues examined, this article will touch upon governance, procedural, substantial and technological matters.

2. The impact of the jurisidiction and of the *locus commissi delicti* principle on the governance of cybercrime investigations

The Cybercrime Convention was implemented in Italy by Law No. 48/2008[10]. Practitioners quickly realized it did not neatly solve the growing problem of the strong extra-territoriality nature of cybercrimes. Years after its implementation, some scholars[11] called for a reform of the Convention as the jurisprudence was struggling with the existing framework. Between 2008 and 2009, a controversial case tried to address the problem of whether Italian authorities could claim jurisdiction over a website offering its services in the territory but using servers located abroad. The case concerned alleged copyright infringement by the peer-to-peer Swedish platform *PirateBay*[12]. An Appeal Tribunal ruled in September 2008 that, in spite of no evidence of Italian citizens committing the crime, jurisdiction of Italian prosecutors would still apply, although it was not lawful for such authorities to perform a so-called "internet

traffic hijacking" as part of the concept of "seizure" under Art. 19[13] of the Convention. This interpretation was then reverted with a decision of the Italian Supreme Court (*Corte di Cassazione*)[14], which reintroduced the notion of internet hijacking as a technically feasible measure, while still confirming the Italian jurisdiction over such a case[15]. In 2013, the Belgian Supreme Court (*Cour de Cassation*) equally confirmed the lawfulness of a far-reaching injunction order, based on the national provision on seizure of computer data[16], against all Belgian Internet service providers, requiring them to block access to IP rights-infringing content hosted by a server, linked to a specific main domain name, by employing all possible technical means at their disposal or at least by blocking all domain names that refer to a specified main domain name ("thepiratebay.org")[17]. The Court ruled that "appropriate measures" to render data inaccessible can also be addressed to third parties (and not only those who store the data and have them stored), and that data seizure can also be used as a preventive measure, to secure private interests (*in casu* the interests of copyright holders), and not only for fact-finding reasons[18].

Jurisdiction issues do not only affect search and seizure within the realm of the Convention. Beyond Art. 19 of the Convention, the cross-border feature of cybercrimes and the evolution of criminals' *modus operandi* have also influenced the determination of the *locus commissi delicti*[19] principle and the correlated governance of public prosecutors. The issue of finding efficient and effective governance models to fight cybercrime is not something new nor unusual. Over the years, many have suggested multiple models, not least what somebody called "Uberisation"[20] policing, participative governance which builds upon cooperative networks and information exchange with private businesses.

Generally speaking, rules of attribution within the Italian jurisdiction are included in Articles 6 to 10 of the Italian Criminal Code (hereafter, C.C.). Under Art. 6, individuals are punishable under Italian laws for any offences (wholly or partly)[21] committed within the Italian territories[22]. Although few provisions in the C.C. may derogate from it, such as in the case of association with terrorist finalities (Art. 270*bis*)[23], the general rule incorporates the adoption in the Italian criminal law system of the *ubiquity*[24] principle. Such a notion is a combination of three criminal law theories for the allocation of jurisdiction, namely *physical act* theory, *instrument* theory and *result* theory[25]. Accordingly, under the ubiquity notion, it suffices that a fragment of the perpetrators' conduct has taken place on Italian soil.

Nonetheless, the theories above cannot be considered fully harmonized across the European continent. On the one hand, the ubiquity theory also applies in Belgium, for instance, where the "hidden extraterritorial application"[26] doctrine allows Belgian courts to be territorially competent for crimes committed abroad if there is an indivisible link between the offence and the effect of it[27]. Conversely, a number of states also consider non-constitutive elements of the offence as variables to take into account when defining territorial jurisdiction. For instance, in the 1993 United Kingdom's Criminal Justice Act, the interpretation of "relevant event" influencing the jurisdiction process seems to be broader than both Italian and Belgian examples, defining it as «(...) any act or omission or other event including any result of one or more acts or omissions». This wording extends the scope of British criminal prosecution by including in this conceptualization *non-constitutive elements*, such as «preparatory acts or non-constituents effects»[28].

Having said that, it is noteworthy to look at the powers of the public prosecutors in Italy. In particular, Art. 11 of Law No. 48/2008 added paragraph 3*quinquies* to Art. 51 of the Code of Criminal Procedure (hereafter, C.C.P.), introducing a delocalization principle in the establishment of prosecutors' offices for computer crimes. This geographical delocalization was implemented in order to allocate the powers arising from Art. 51.1(a) to the public prosecutors' Office of the District Court where the corresponding competent Judge is established. This process seems to mirror Law No. 8/1992[29], which includes measures to enable a coordinated response to mafia crimes, *inter alia* the establishment of the Anti-Mafia National Directorate (in Italian *Direzione Nazionale Antimafia*) to counter mafia-related organized crime through a top-down investigative approach which soon took the name of "anti-mafia prosecution service".

However, the above-mentioned delocalization principle imperfectly echoes the Anti-Mafia governance system, as Law No. 48/2008 does not entirely set the basis for the establishment of a centralized Coordination Directorate on Cybercrime (gathering experienced public prosecutors and investigators). This incomplete parallelism results in a number of major challenges for law enforcement cybercrime officers. Differently from the anti-mafia law, it does not fully follow the same top-down governance model, endorsed for its efficiency and effectiveness in delivering results through a capillary yet well-structured system[30]. The approach towards Law No. 48/2008 results in return in a lack of channels and mechanisms for the exchange of common investigative best

practices, therefore leaving a rather local approach towards cybercrime investigations, sometimes solely handled by district-based units. This creates a loophole in the systematic establishment of coordinated investigative techniques, an issue that is worsened by the increasing trans-national nature of computer crimes. Law No. 8/1992 has in fact proven to be effective over the years thanks to the implementation of a proper roster of prosecutors solely dedicated to countering mafia-related crimes within the whole judicial hierarchy[31]. Conversely, such levels of efficiency and efficacy cannot yet be achieved in the context of Law No. 48/2008, due to the non-coordinated response to cybercrime, particularly with a view to a fundamental lack of long-term strategic approach, leading to scarcities in resource allocation and capacity building[32].

These imperfections in the governance of prosecutors' offices might lead the investigator to potential failures in gaining an understanding of the full picture and the broader criminal intent[33]. This is proven particularly true over the recent years, where, in parallel, more and more cybercrime operations are showing how criminal networks are dismissing their highly hierarchical top-down structure (typical in many offline organized crimes) in favor of a more horizontal and distributed online model. This is mostly the case for financial cyber frauds and the like, where big gains can be achieved by a collaborative, egalitarian model with only few masterminds behind it and a broader network of executers. Such structure, combined with the afore-mentioned extra-territoriality nature of cybercrimes, makes the life of investigators and prosecutors even harder. In Europe, this deficiency is sometimes overcome by the increasing coordination role of supra-national organizations like Europol, as confirmed by the findings in the aftermath of operation *Carbanak*[34] (a number of cyber-criminals arrested over Europe with the charge of financial frauds), which gathered for a long period of time investigators and Joint Investigative Teams from all over the continent and beyond, at the same time revealing how such types of distributed networks of criminals operate today.

The examples above show how the intersection of domestic criminal law with international provisions on cybercrime have an influence on the establishment of the competent jurisdiction and the governance of prosecution. These issues have a broader echo if combined with the trans-national shape of crimes committed online. Observers are still bringing forward the argument that countering computer crimes is particularly challenging due to a substantial governance gap[35]. As we will be able to see below, the Convention nonetheless opens up to a number of interpretative issues with reference to even more practical investigative matters, too.

3. Seizure, acquisition and transfer of electronic evidence

The topic of e-evidence is largely debated in digital forensics. The following section will approach current legal and interpretative issues behind the seizure of private and confidential communication, open source information and metadata, including their transfers for investigative purposes. As we will be able to see, concerns are only partially related to the Convention and its interpretation. Rather, all issues analyzed are part of a broader impasse healed by a number of factors, including the reform of the European Union's data protection legal framework[36] (expected to provide for more stringent rules for law enforcement access to digital data[37]) and the difficulties of having to cope with multiple jurisdictions in cases of prosecution of cross-border criminal activities.

Legal certainty within domestic legislations should be sought by looking at a number featuring elements, starting from the basic definition of digital information and digital data. Depending on the context, in the Italian jurisdiction the term "digital data" could imply two different meaning at least. First, it can be assimilated to the notion of "electronic correspondence" (email). Second, within the administrative law domain, it could be used as a synonym for "digital document" (i.e., in principle, excluding correspondence), defined as "the representation of acts, facts or legally relevant data"[38]. As we will be able to see, this distinction has an important procedural consequence with respect to the seizure of electronic correspondence. The following sub-paragraph will explain what is the discipline for the seizure of electronic correspondence as opposed to digital document. It will be described how investigators could include in the second meaning also those emails who can be categorized as non-read, thus applying the discipline of seizure of non-correspondence. It will show how this could be particularly advantageous for the cyber investigator, as it could benefit from the non-discovery of this investigative act (and of the investigation) to the suspect. The application of the two regimes has therefore a different impact on the due process rights that are reserved to the suspect of a crime which is investigated by law enforcement.

3.1. Seizure of electronic correspondence and the international reforms on e-evidence

In the Italian jurisdiction, the procedural and administrative checks and balances disciplining a data seizure often undermine the effectiveness of this instrument, let alone under the applicable framework arising from the implementation of the Cybercrime Convention[39]. The Italian interpretation for the notion of correspondence comes, *inter alia*, from the Supreme Court[40], where the term is defined as «(...) a dispatch activity in progress or begun throughout the handover of the envelop (...) for the delivery». From this reasoning, it is presumed that in the above circumstance the sender has not yet consulted the message. In the online setting, the established Italian system for the legal validation of electronic correspondence called PEC (certified electronic correspondence, which, according to its constitutive act – Presidential Decree No. 68/2005 – offers a legal guarantee of the integrity of the email) implies the introduction of timestamps from the service provider in both the moments of the sending and the receipt of the message, certifying the correct flaw therein. Some compare the case of a sender who does not digitally sign a message to the case of a registered paper mail that is left to the concierge or to the competent postal office situated in the proximity of the receiver.

Having said this, the seizure of electronic correspondence in a purely Italian setting normally starts[41] with the inhibition from the subsequent submission of those messages, subject to certification activity from the Italian PEC service provider. In contrast, the seizure of foreign services can only happen under two circumstances: (i) international cooperation[42] and (ii) *digital* search[43] under the defensive safeguards arising from the rights of a fair trial and due process[44]. It needs to be noted here that the cyber investigator is duly constrained by the constitutional right to private correspondence[45]. Looking at such principle from a data protection perspective, it thus becomes challenging to appropriately address the purpose limitation[46] principle (for which only necessary data is to be processed) by just querying the mailbox service with keywords that may refer to various parts of the message (header, body, attachment), without potentially interfering in the processing of irrelevant (non-pertinent) content or metadata[47].

Moreover, the Italian legal framework seems to contemplate only those cases where the recipient of the message is using the old-fashioned POP3 protocol[48] which, in its basic configuration, allows to free the e-mail server from the messages once they have been downloaded by the client. The modern practice enables instead the temporary storage of a copy of the messages (with a disposal policy of three days, for instance) or permanently (by using the IMAP protocol[49]), until these are deleted by the client side. Under this circumstance, and unless there are particular configurations of the IMAP server (for instance, the "store" setting), how would an investigator be able to determine whether a message has actually been consulted by one party, but then reconfigured to be shown as a non-read mail? It is clear that the issue is not a purely normative one, as it includes strong technical considerations, too. Parallel discussions were brought up by other scholars and in a number of various jurisdictions, such as in the United States of America[50] or in Belgium. For many years, Belgian courts and legal scholars have intensely discussed the best method to discern a read message from a non-read one, as well as how to legally qualify various situations of "data at rest" and "in transmission" in order to determine on the basis of which legal ground a warrant had to be produced by either the public prosecutor or the examining magistrate (investigating judge): on the basis of network search, or interception...?[51] Finally, in 2016, the Belgian legislator put an end to the discussions by significantly broadening the scope of the provision on interception[52]. Whereas the old Art. 90*ter* on wiretapping allowed, under certain circumstances, investigating judges to issue a warrant "to listen to, gain knowledge of, and record" specified private (tele-)communications "during the transmission thereof", the new Art. 90*ter* allows the "interception, gaining knowledge of, search and recording" of specified "communications or data which are not publicly accessible". The deletion of the phrase "during the transmission" has rendered the discussion about whether data are at rest or in transmission irrelevant.

Drawing from such experiences, and on the basis of the above mentioned decision of the Italian Supreme Court[53] on the notion of correspondence, it becomes clear that a further clarification on the definition of message "consultation" is of extreme importance, both at the Italian and at the international level, where basic concepts on cybercrime and digital forensics could be harmonized by gaining a commonly accepted meaning throughout all the ratifying jurisdictions. Nonetheless, Italian prosecutors may still acquire the content of a mailbox by ways of Art. 254*bis* C.C.P. (*seizure of digital data from internet or telecommunication service providers*), as opposed to the general provision of Art. 254 C.C.P. In this case, they would then consider a non-read message as digital data (or digital document), with

a number of consequences. Whilst the general Art. 254 does not mention any duplication of the data, Art. 254*bis* instead specifies what actions are required from the service provider in order to ensure the retention, handover and duplication of the data. For this reason, the importance of a clarification on the email-consultation matter described above is further supported by the fact that the cyber investigator has to rely on the term "document", as opposed to "correspondence", in order to *de facto* enable the application of Art. 254*bis* C.C.P.[54]. The choice of preferring Art. 254*bis* is made on the basis of two main arguments. First, because it ensures a non-discovery of the ongoing investigation, since the provider is solely required to handover a copy of the data stored within its servers without having to subsequently deny the access of such data to the recipient of the communication. Second, such preference is made in order to avoid the authorization procedures for the interception of an Italian-based mailbox by the so called "incremental seizure"[55]. This type of confiscation furthermore opens up a substantial conflict with the non-repeatability of the seizure itself, due to its "surprise" nature: it still remains unclear how is it possible to comply with such an important element if the activity can be reiterated over multiple dissociated timeframes.

It was said above that the use of international cooperation mechanisms is one of the two cases under which a foreign seizure could be undertaken[56]. At the time of writing, some legislative reforms are being discussed within the European Institutions[57] with regards to a new pan-European framework on e-Evidence[58], and are expected to be turned into law sometime after the end of the 2013-2019 Digital Single Market Strategy. The push for a reform of the e-evidence framework derives from the time-consuming procedures currently in place in the law enforcement cooperation domain, in particular with reference to Mutual Legal Assistance Agreements Treaties (MLATs): «law enforcement and judicial officials often consider the procedures for judicial cooperation as too slow, disproportionately cumbersome also in view of the limited interest of the receiving country, and thus inadequate»[59]. While waiting for such stronger common European initiative to address these points, and in order to avoid such long waiting times often proving detrimental to the investigation, the Italian judiciary police keep acquiring data by virtue of Art. 247.1*bis* (*delegated digital seizure*) or Art. 351[60] (in case of flagrancy, *ex officio*) while still respecting the due defense rights to a fair trial[61].

The initiative of the European Union, however, is not the only one trying to address such issues. On a greater level, the Council of Europe's ambition to update the Cybercrime Convention thoroughly touches upon the harmonization of the handling and exchange of electronic evidence. Amongst others, the draft protocol includes a revision of the MLATs instrument, with the inclusion of an expedited form of "emergency MLATs". Such an instrument, which could be triggered solely in the event of an imminent risk for one or a group of individuals, would address urgent cases where rapid responses are needed. Much work still needs to be done in this respect, as for the time being, not many details have been uncovered with regard to the exact definition of the cases when the Emergency MLATs could be used, paving the way for a risk of misuse of this instrument by law enforcements and agencies the like, in the absence of specific definitions on the matter, which would provide for legal certainty on the proportionate invocation of such clause by the above-mentioned actors. The initiative, however, outlines how different lawmakers at different levels have become attentive on the issue. Whilst an EU push on e-evidence harmonization could be considered as a relevant initiative, the Council of Europe-led reform of the Cybercrime Convention would definitely be a much wider forum for standardization and mutual recognition. The Convention continues to set out the standard rules for cybercrime legislations in more than sixty countries, and for this reason the efficacy of its provisions could be welcomed at a greater stage. In the meantime, what comes out as an underlying need from a legal and policy perspective, is the hope for an efficient harmonization of both procedures and human rights' safeguards between the EU and the CoE levels and their respective proposals.

Therefore, while an international move towards codification is being observed, the legal fragmentation in the field still persists (as demonstrated above) within and amongst countries[62].

3.2. Acquisition, exchange of foreign data and the concept of open source

The need of an harmonized approach between the European Union and the non-European members of the Council of Europe offers us the chance to look deeper at how the acquisition of data from the United States is dealt with by the Italian authorities. The reason for undertaking such an analysis is the continuous interaction between the United States and European countries in terms of data transfer. The following analysis will study the combination of both American and Italian legal frameworks, highlighting some of the legal loopholes therein, risking to jeo-

pardize both the investigation of criminal activities and the protection of personal information in the cyber sphere. *Inter alia*, this section will also analyze the concept of open source data as developed by the Italian jurisprudence.

3.2.1. The Yahoo! case

It useful to start, however, with a brief description of a landmark case which took place in another EU Member State. European countries seem to have different standards for distinguishing between national and foreign service providers. By referring to a notorious jurisprudential case that we will soon mention, Depauw[63] states that «Whereas some member states refer to the main seat of the service provider, other use the place where the services are offered and the place where the data are stored, or even a combination of alternatives». A Belgian case which attracted world-wide attention was the *Yahoo! v Belgium* "saga"[64], which unfolded when Yahoo! refused to comply with a Belgian public prosecutor's request (based on Art. 46*bis* of the Belgian Criminal Procedure Code) to hand over the IP addresses associated with e-mail accounts registered to Yahoo!'s e-mail service. Yahoo! Inc, domiciled in California, developed two main lines of argumentation. Firstly, that Belgium was imposing its criminal laws extraterritorially and, secondly, that it did not qualify as an "electronic communications provider" in the sense of the Belgian Code, and, therefore, not obliged to disclose identification data to the public prosecutor. The legal procedure ran from 2007 to 2015, and the Belgian Supreme Court (*Cour de Cassation*) had to intervene not less than three times. In its final judgment of December 2015[65], it upheld the Antwerp Court of Appeal's view[66] that Yahoo! is territorially present in Belgium, hereby voluntarily submitting itself to the jurisdiction of the Belgian authorities: it takes an active part in economic life in Belgium, among others by use of the domain name http://www.yahoo.be, the use of the local language(s) on that website, pop-up of advertisements based on the location of the users, and accessibility in Belgium of Belgium-focused customer services (among others: a "Belgian" Q&A, FAQ, and post box)[67]. The Court of Appeal of Antwerp had concluded that the accusations of extraterritoriality could only be invoked and accepted had there been a request for the handover of data or objects which are located in the USA, with which there is no Belgian territorial link whatsoever, and if the holder of these objects or data is not accessible in Belgium (either physically or virtually)[68], thereby, applying to the extraterritoriality principle.The Court of Appeal applied the same line of reasoning in a case involving Microsoft's online communication service Skype. The Court also rejected Skype's claim that it did not have the technical capability to comply with the request for wiretapping[69].

The issue at stake has a broad connotation when establishing jurisdiction for data access in the cloud, which, accordingly, is under discussion within the auspices of the Cybercrime Convention reform[70]. At other national levels, similarly *broad*[71] interpretations can yet be different than the Belgian case. To name two examples, while in Argentina jurisdiction is established by the place where the trial would take place (hence, following a rather deeply fundamental criminal law approach)[72], Brazil extends its jurisdiction even further, including in it data collection, processing, transition and storage taking place in the country[73]. Although slightly different one another, all of such national examples collectively seem to confirm the most recent doctrine, holding that «territorial regulations are increasingly having an outsized territorial effect»[74], and the reason for this is to be found in the international feature of the companies retaining the information. The examples above add up an element to this consideration, whereby this effect does not only apply to current regulations, but also to their enforcement by investigative and judicial authorities. From a governance perspective, this element furthermore supports the view that this form of unilateral rulemaking[75] represents a way for nation states to claim their sovereignty (and their jurisdiction) against a more multilateral and multiparty approach characterizing the various layers that compose the cyberspace[76].

3.2.2. Data held overseas and open source data

As suggested by facts at stake in the *Yahoo! case*, during a cyber-investigation, police officers often find themselves in the condition of acquiring content data or log data (metadata) stored on servers located in a foreign country. Since the majority of the service providers store the data in the United States[77], the normative framework of reference for the execution of such an investigative activity is the Electronic Communications Privacy Act (ECPA)[78], Title 18, which foresees three procedures.

Firstly, backup preservation[79], aimed at preserving (without delivering), both content and metadata for a fixed period of 90 to 180 days.

Secondly, voluntary disclosure[80], which can be carried out in two ways: emergency disclosure[81] and

domestic legal process (for all other cases and solely aimed at obtaining metadata).

Thirdly, Mutual Legal Assistance Treaties, i.e. throughout agreements – normally bilateral conventions – of mutual assistance, to be executed via the application of established international cooperation plans. In such circumstances, access is possible with a search warrant[82] that allows the acquisition of a larger number and variety of data, such as metadata, content data and cross-border traffic data.

Once acquired by the Italian investigators, data will be lawfully obtained and admissible if procedures will be compliant with both the Italian Data Protection Code[83] and the Code of Criminal Procedure. However, some gaps between the American and the Italian laws might reveal a much broader set of issues deriving from a number of legal uncertainties.

With regard to the Italian Data Protection Code, Art. 132.4*bis* deals with the request for data preservation, which differs from the American normative counter-part in the definition of both recipients and category of data. Whilst in the United States such provision addresses service providers (operators offering generic services), in Italy the specular norm solely addresses electronic communication service providers (*fornitori di servizi di comunicazione elettronica*), alternatively called "access providers"[84]. As far as the type of data is concerned, the American legal framework considers within its scope both content and metadata, while the Italian norms solely refer to the latter typology, leaving out the content of the communication in respect of the principle of confidentiality.

Regarding the Italian Code of Criminal Procedure, Art. 234*bis* refers to the acquisition of data from both open source and "legitimate owner"[85]. Such norm mirrors Art. 32 of the Cybercrime Convention[86] (which mentions open source data), but was introduced within the Italian criminal procedural system under urgency regime. Such a provision was then confirmed within Art. 2 of the Law No. 43/2015[87], which in turn draws from the UN resolution No. 2178[88] concerning the upsurge of the so-called "foreign fighters"[89]. Under these auspices, the Italian legislator has not clearly defined a number of crucial terms, including the meaning of open source, as it will be shortly explained.

The Cybercrime Convention mentions "publicly available data" under Art. 32 by confirming the lawfulness for a Country to «access publicly available (open source) stored computer data, regardless of where the data is located geographically»[90], as well as «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.»[91].

In Europe, a number of jurisdictions have implemented Art. 32[92]. Interestingly, in many of them, the terms "open source" and "publicly available" data are in principle used interchangeably. Notwithstanding such an overlap, interpretations of Art. 32 may still take diverging avenues. Koops[93] explains that under the Romanian cybercrime legal framework, it is made expressed condition for the applicability of Art. 32 that computer data *and* its source (emphasis added) are public. This may suggest a discrepancy between an information and its source[94]. Consequently, under such a framework, the notion of public availability has a twofold characteristic: public access to the data by the general audience on the one hand, and an inherent feature of the data itself (i.e., generated in the public domain, publicly broadcasted, and so forth)[95] on the other. Nevertheless, scholarship has not been so much more involved in explaining Art. 32 and its effects, even though a number of interpretative issues on public availability are still unresolved, for instance with regard to state sovereignty in an open-source internet search[96] or in respect to the applicability of data protection laws for publicly available data[97]. With respect to the latter, a number of scholars seem to agree that it is not only a mere assessment of the public availability of the data that helps defining the privacy intrusion, but also the level of automation and retention of the data collection itself play an important role as additional criteria for such an assessment[98].

As we see from these few yet clear examples, doctrine[99] and the law[100] have yet not agreed on a commonly accepted definition of open source data and its implications. Attempts to define it often draws from a negative approach, i.e. delimiting the concept by explaining what is not[101] an open source information.

In the Italian framework, we can try to derive such concept from both law and jurisprudence. A general definition comes from the Code of the Digital Administration, Articles 1(n) and 1(o)[102], whereby publicly available data is defined as an information that is identifiable to anyone. A narrower definition of open source is instead given under the criminal law context. It originates under the auspices of the jurisprudential evolutionary interpretation of the notion of "public space"[103] as a standalone notion, opposed to the one definition "space open to the public"[104]. By consequence, within the notion of "non-publicly available data" under the Italian legal framework,

we may even include all data protected by any "security measure or access control" intended as technical software measures[105] (e.g. password), suitable to address the so-called *jus excludendi alios*[106]. However, there are certain practical examples under which the Italian jurisprudence has not clarified the conditions under which open source data can be freely and lawfully investigated yet, such as when data are non-*indexable* by search engines (for instance, through *robot.txt*) but are nevertheless acquired via direct access to the web server folder (not password-protected). From a merely subjective point of view, such a condition could demonstrate the deliberate willingness of the data subject to exclude access to his or her data solely through specific technical measures focused on search engines. Nonetheless, this may not in principle exclude that the same data can be freely accessed by an ordinary query, which makes it difficult to think of such a measure as suitable to expand *erga omnes* the right to privacy[107].

3.2.3. Legitimate owner

Another point of concern is the definition of *legitimate owner* (i.e., «the person who has the lawful authority to disclose the data») according to Art. 32 of the Cybercrime Convention. Such a notion cannot be tidily matched with the one of "data controller" under Art. 4(f) of the Italian Data Protection Code[108], neither with the one of "creator" or "possessor" of the data (which in turn can be, under certain cases, matched with the person of the inquired himself). Notwithstanding that very little time has been dedicated to the conceptualization of Art. 32 of the Convention[109], a short case study might clarify why at both national and international levels, approximation of laws and clarifications on such definitions would be welcomed by the digital forensic community. Take for example the following scenario: Mario produces a photo which is shared with Giulia via WhatsApp; Giulia uploads the picture on her Dropbox cloud service. Who is the "legitimate owner" that will have to be addressed by the cyber investigator for the handover of the file stored within the digital domicile of Giulia? The person who produced the file (Mario), the person who handles it (Giulia) or the entity who stores it (Dropbox)? All such questions seem to remain unanswered at both international and national levels.

3.2.4. Further issues on Art. 32 of the Cybercrime Convention

With reference to the clause of Art. 32 *data stored abroad*, i.e., within a physical or logical territory which is not included in the jurisdiction of a country, the interpretation of the Italian jurisprudence does not allow us to define what areas are "different from a state's territory".

For instance, questions arise on those logical environments created by a *cloud service* paradigm, which normally allows the identification of the legal person handling the data, but not always its physical storage[110].

The impact of such an approach was reflected in a recent decision of a U.S. Appeal Court from the 14 July 2016 and heard before the Supreme Court on 28 February 2018[111], where American providers communicated that they would not be able to produce digital data any longer if such data were not physically stored by servers located on U.S. soil. The case is about a controversy between the United States Government and Microsoft[112], after a refusal from the company to hand over content information associated with an email account where data was physically stored in a non-U.S. based server. While the decision of the Supreme Court determined that there was no longer a matter to adjudicate and ended the proceeding following the adoption of the CLOUD Act[113], the United States Court of Appeals for the Second Circuit had previously ruled in favor of Microsoft, invalidating the injunction from the U.S. Government, aiming to receive a number of emails from an account which server was located in Ireland. It needs to be mentioned here that, Microsoft interpreted American SCA (Stored Communications Act)[114], as not forcing companies to hand over content data (e.g., emails), rather only subscriber information. Pursuing harmonization purposes, there is a growing argument saying that such a tiered approach could potentially be the same one explored in both the e-evidence reforms by the Council of Europe[115] and the European Union[116]. Layered data protection standards might be therefore envisaged within, where both texts will foresee an easier access and transfer by and between governmental agencies in the case of subscriber data, as opposed to content information such as emails or messages. On a domestic level, this will presumably mean that criminal law provisions will have to ensure a stronger set of safeguards for the transfer of the latter typology of data, by ways of more stringent judicial reviews and authorizations as well as strict security measures when the transmission takes place. However, whilst this approach might ensure an expedited channel for the exchange of subscriber information amongst law enforcement, helping the resolution of urgent and compelling cases, the differentiation between content data and metadata might generate perplexities from a data protection stand-

point. As stated by the jurisprudence of the European Court of Justice in the landmark Digital Rights Ireland[117] and Tele2 Sverige[118] cases, although there is an actual difference between the two types of data, both of them are substantially equal in their sensitive nature from the perspective of the right to data protection[119].

Furthermore, it is worth noting that none of the main jurisdictions under scrutiny in this section (Italian or American) have a mechanism in place for the coercive acquisition of foreign data with strong fair trial safeguard, nor they have in place instruments applying the so-called "digital seizure" (Articles 247.1*bis* or 352.1*bis* C.C.P.) to foreign data. As said above, the Italian legislation does not explicitly mention the possibility to access and acquire forcibly such data, neither in presence of the counter-part (thus complying with the right to fair trial and adversarial principles). Such an activity is often undertaken by Italian law enforcement agencies according to the attribution principles under Articles 6 to 10 of the C.C.[120].

While the Microsoft Case is coming to an end, the United States' Government has also decided to rapidly reform its legal framework on the transfer of e-evidence. U.S. lawmakers are aiming to ease the exchange of users' data stored in servers respectively located on the U.S. soil and in the territories of the European Union. The newly adopted CLOUD Act[121], will in fact authorize American law enforcement authorities to demand U.S. companies with European-based servers to hand over data of users involved in a federal investigation without the need of an MLAT, and on the basis of executive bilateral agreements with Member States[122]. Taking into account that the bill raised criticisms by civil liberties groups and privacy advocates[123], it is worth noting that the United States' Government is not the only executive branch receiving a fierce opposition against such initiatives[124], as much clamor has been raised across the European Union with regard to continental reforms, too.

4. Retention, NAT techniques and deletion of data

Notwithstanding the use of lawful anonymization techniques on the internet, such as proxies or similar PETs, tracking activities online are often constrained by a combination of legal[125] and technological boundaries. As briefly mentioned above, in Italy the cybercrime investigator generally obtains online traffic data by ways of formal notification to the ISP signed by the prosecutor. Among the legal constraints, issues arise from the non-certified identification of the owner (consumer) of the internet contract. Voice and data telecommunication contracts are regulated by the Italian Code of Electronic Communications[126]. Art. 55.7 states that any electronic provider is required to handover its data on users holding a contract or a pre-paid arrangement with them, which implies that customers have been identified at the moment of the activation of the service. Such data needs to be made available to the judiciary authority, which shall have the faculty to access that data for criminal justice purposes.

However, the said Code includes a number of interpretative issues with respect to two main points. Firstly, it does not explicitly specify the minimum standard steps to validate and verify that the holder of the telephone contract is actually the person who he or she claims to be at the moment of the activation. Secondly, no specific sanctions seem to be envisaged against the operator that does not respect such provisions.

To fill in such loopholes, a new Italian data retention framework has been recently introduced by way of Law No. 167/2017[127]. The need for a reformed regime comes from the legal vacuum left by the invalidation of the so-called Data Retention Directive[128] by the EU Court of Justice in 2014[129], and the subsequent cases that followed the decision[130].

However, with a view of such European decisions, the Italian legislation raised someone's eyebrows for a number of elements, namely the length of retention periods (forcing service providers to retain internet and traffic data for six years), and fact that the request received is signed by the public prosecutor alone. Taking into account that only a few European Member States have such lengthy retention periods[131] now in place (the invalidated Directive had a 24 months as a maximum threshold), and bearing in mind the arguments of the Court of Justice in 2014, it would not come as a surprise if Law 167 might be soon scrutinized in its necessity and proportionality by a court of law.

Furthermore, amongst the technological constraints for cybercrime operators, NAT (Network Address Translation)[132] techniques are becoming a growing impediment for the identification of IP addresses belonging to IPv4[133] family. Such an issue has not only been voiced by the Italian investigators. Europol has recently advocated for a restriction of IP-sharing via CGNAT techniques, too[134]. NAT technologies are deployed by Internet Service Providers to compensate the incremental absence of available IPv4 addresses to give to customers trying to connect to the internet at any given moment. In

some circumstances, such a solution turned out to be a proper counter-forensic technique, as it does not allow the unique identification of the contract holder as foreseen by Art. 5 of the Legislative Decree 109/2008[135], forcing cyber investigators to analyze a multitude of potentially relevant users. Such a risk can be mitigated if the tracking is performed *ab origine* (from the very beginning) by content providers (e.g. YouTube, Twitter, Facebook, etc.), via the gate number of the internet service under scrutiny. However, for the law enforcement community such a way of addressing this issue encounters two main constraints. First, content providers do not normally offer this type of information, as no legal requirement exists that forces them to do so. Second, norms arising from the EU privacy reform package, namely GDPR[136] and Police Directive[137], are likely to prevent[138] the indiscriminate collection of personal information by content providers themselves.

Lastly, at the end of the investigative and trial activities, it often happens that the seized object is subject to "seizure and deletion"[139]. The application of such a measure, aimed at the expropriation of intangible elements like digital data whilst returning the storage medium, is a difficult challenge for the cyber investigator. State of the art technology solely allows a circumscribed and reasonable deletion of a file, which can still be available, in another storage medium or uniquely distinguishable by a hash code (e.g. MD5[140] and/or SHA-1[141]). This reasoning derives from the assumption that the nature of digital data cannot exclude that the same file be stored elsewhere, for instance in different storage medium than the one seized (USB-drives, SD cards, hard disks) or in the same medium which was subject to seizure, because present in other mediums in the meantime.

5. Forensic examinations: repeatability, forensic experts and technical measures

When transposing the Cybercrime Convention, the Italian legislator missed the opportunity to amend the Italian Code of Criminal Procedure regarding forensic examinations. The following section will analyze this issue and a number of correlated instances. It will elicit the links between the need for further clarification in the forensic examinations domain, and the missing link with the implementation of the Convention. In particular, three issues are raised and discussed hereby: the uncertainties in respect to the repeatability of forensic examinations (and the challenges of ensuring due process rights throughout such proceedings), training profile of forensic analysts and judicial bodies and lastly, the definition of the term "technical measures" within the Italian cybercrime normative and jurisprudential framework.

The C.C.P. includes three different instruments to conduct forensic analysis, namely technical forensic examination, motions for expedited evidentiary proceedings within preliminary investigations and assessment by court-appointed technical experts during the trial proceedings (respectively pursuant to Articles 359 and 360, 392 and seq., 220 and seq. of C.C.P.)[142].

With regards to the first group, in the event that technical examinations are to be conducted on individuals, object, or places that are subject to modifications ("unrepeatable examinations"), the public prosecutor has to notify in a timely manner all the parties and the defense counsel of the date and time when such examinations are due to take place, as well as the possibility for the parts to nominate a technical expert[143]. In particular, Art. 360 refers to those examinations that, due to the mutable status of the subject or object to be verified and the potentially disruptive nature of the activity towards to object under scrutiny, can only be undertaken once. Think of the examination of a unique DNA sample or a body tissue, which often leads to the incontrovertible destruction of the evidence after the test: such an assessment can happen one time only before its status changes. Due to this mutable feature, the evidence is considered to be acquired and admitted to court immediately, thus prior the beginning of the trial phase (where the admission of an evidence is normally assessed), with the consequence that the judge will be able to fully consider that examination to base its decision. For this reason, due process rights and adversarial principles need to be guaranteed during this particular process of evidence acquisition[144].

With a view to the fact that such a provision would apply to both offline and online scenarios, Law No. 48/2008[145] surprisingly did not modify the text of Art. 360 C.C.P. (titled "technical forensic examinations") which, in the context of cybercrime, is often invoked when there is a significant risk of tampering, alteration or damage of data, information or information systems, and a subsequent notification of the verification to the parties involved in the proceeding.

It is worth saying however, that scholarship and jurisprudence often question whether the nature of e-evidence might exclude their unrepeatability nature[146]. Again Vaciago states «There is no scientific justification to consider any forensic examination un-

repeatable, if the digital evidence in question consists of a bitstream copy that qualifies as a certified true copy of the original data, as established on the basis of the related hash algorithm»[147].

Notwithstanding the above considerations, the application of such a provision is often difficult in the case when the investigation is carried out against unknown individuals[148] (for instance, in the context of a child pornography investigation), while a simultaneous seizure of an electronic device from an identified subject takes place. In such situations, the adversarial guarantees of fair trial and due process seem to suffer of some legal uncertainty. To simplify, we can think of a case where an individual's device is seized but the person does not have the quality of suspect. From a literal interpretation of Art. 360, such an individual should not in principle take part in the examination. The drawback is that of being excluded from the exercise of his right to defense and due process[149], which may then lead to imbalanced situations in case evidence is found against him on the device. For this reason, the prosecutor is often bound to apply a jurisprudential orientation deriving from a decision[150] of the Italian Supreme Court, according to which the prosecutor is authorized to proceed with the examination pursuant to Art. 360 C.C.P., to inform not only the suspect but also the party against which in that phase there are only leads of having committed a crime. The adversarial setting that needs to be guaranteed, according to Art. 111 of the Italian Constitution[151] has therefore not been addressed by any provision transposing the Cybercrime Convention, forcing prosecutors to rely on an instrument deduced from the jurisprudence as opposed to an established legal framework. This reveals a missed opportunity for the Italian legislator to fill in the gap created by the legal loopholes therein.

Art. 360 is included in Title V of the C.C.P. (*powers and activities of the public prosecutor*). Conversely, the Judiciary Police's activities are instead enlisted in Title VI. The Judiciary Police should be entitled to carry out examinations only in the case of necessity and urgency (in Italian *necessità ed urgenza*), which is further explained by Art. 354 C.C.P. by the term *indifferibilità*, i.e. when an event cannot be postponed or repeated. Therefore, as a general rule, Judiciary Police is not entitled to carry out an examination *sua sponte*, but only under the mentioned extraordinary circumstance. However, two elements need to be noted here. Firstly, this practice is often overcome by the application of Art. 370[152] C.C.P. by ways of accustomed principles. Secondly, pursuant to Articles 392 and seq. of the C.C.P., the instrument of expedited evidentiary proceedings allow for a forensic examination with an adversarial setting to be held in both preliminary investigations and preliminary hearings[153] (i.e. "after charges have been formally brought"[154]).

Having said that, doubts also relate to the identification of the expert in charge of performing the technical examinations. This consideration mostly pertains to the procedural obligations arising from the assessment by a court-appointed technical expert (for example, pursuant to Articles 220 and seq.). First and foremost, it is worth saying that technical experts on computer forensics are quite a relatively new category in the judicial sphere[155]. Moreover, generally speaking, the findings of the expert need cross-examination by an expert witness at trial before they are declared admitted[156]. A number of unresolved questions still persist however with respect to what certified technical skills he should have as a pre-requisite to undertake forensic analysis and verifications the like. For instance, it is not clear who attests the technical skills of an operator. Specifically, would a simple IT-related degree suffice? Unlike many other thematic areas and sectors (for instance, accountancy), a sworn digital forensic expert that offers his services to the Court is normally required to self-certify himself as an IT expert, with no further assessment on his capacity by the Court itself. According to the rules on the appointment of technical experts, a number of professional categories are explicitly mentioned in the mandatory list of profiles a judge or a prosecutor can choose from to execute any form of forensic activity. Digital forensics, and in particular information and communication technology experts, are not part of such a list, meaning that Art. 67 paragraphs 3 and 4 of the Rules Implementing the C.C.P. apply: whenever a technical expert not belonging to any of the listed categories is to be chosen, the judge's choice is merely based upon his personal assessment, which should be duly grounded. Still with a great part of judicial discretion, though.

The normative loopholes described above bring us to a broader, more internationally-recognized issue: the lack of forensic analysts as well as the poor general knowledge of magistrates and courts on IT forensics matters. Such lack of knowledge worryingly covers all sectors of the investigative and judicial chain: it ranges from evidence-collection personnel to courts and judges deciding on a determined case[157]. This aspect could lead to very diverse interpretations of meanings and characteristics of electronic evidence by judicial bodies, even within the same country. In the United States for instance, issues of surprisingly high standards of electronic evidence ad-

missibility arose in *Lorraine v United States*[158], while it is well renowned among the community of experts the jurisprudential contradiction between the *Maryland* and the *Texas* doctrine on the admissibility of social media evidence[159]. Taking into account a more European perspective, an empirical research was conducted some time ago on the situation of computer forensic experts across a number of EU Member States, including Belgium, Spain and the United Kingdom. Summing the results of such study, it states: «There is an absence of standards (and no legal precepts) setting the characteristics and training that any computer forensics expert must satisfy. The experts themselves consider that basic training is necessary to act as computer forensics specialist: they prefer a degree (especially in computer science, engineering, or mathematics)»[160].

Such an absence is confirmed by the proliferation of sector-specific, local and non-harmonized handling standards, as confirmed by a study from the Evidence project[161] on the status of digital forensics in the EU. Findings of such project revealed a multitude of guidelines and approaches. From an Italian perspective, guidelines are issued by the Digital Forensic Alumni Association, Tech and Law Center Society, DEFT Association, as well as the Milan's prosecutor office (in Italian *Procura di Milano*); a similar situation is encountered in Spain, Belgium and the United Kingdom.[162].

As we can see, this is not only a normative issue. The underlying claim is that training and capacity building across the world still lacks harmonized approaches. A number of projects[163] on judicial training on computer forensics and cybercrime are currently run by many international institutions. For example, the Council of Europe by ways of the T-CY (Cybercrime Task-Force) paved the way for a number of successful policies aimed at preparing courts and magistrates for the challenges of the cyberspace. However, these actions should be going in parallel with a more detailed attention by universities and academic institutions in activating training and courses on digital forensics, in order to educate new generations of forensic analysts[164]. This proliferation could ultimately help filling the value gap between IT experts appointed by the Courts and those hired by the defendants (who normally have to bear the expenses of such performance by themselves, until reversed decision by the judges).

A last concern arising from the Italian example is the introduction of the hybrid term "technical measures"[165] (in Italian *misure tecniche*), which is present in a number of Articles in the C.C.P. with the implementation of Law 48/2008. It should be mentioned that the legislator missed to provide such a reference in Art. 360, too, where it could have been appropriately explained. It is important to note here that the Supreme Court had to rule twice in favor of providing further clarification on the distinction between two slightly different although complementary terms. Such decisions in fact conceptualized the differences between a mere "scrutiny"[166] (i.e., the observation, measurement and description of given sites, individuals and objects which do not imply the study nor critical evaluation of the data therein to the extent that such an assessment does not overcome the sensorial and perceptive dimension of the evaluation itself[167]) as opposed to a more thorough "verification"[168] (i.e., the activity of observation and description of objective elements that leads to critical evaluations). However, while the Supreme Court deemed it necessary to define these two terms, the absence of any specific guidance for a third one, i.e., the above-mentioned wording "technical measure", may lead the cyber investigator to operate within an area of uncertainty as to the instruments and the safeguards available to him. The consequence here is that, due to the missing definition within Art. 360, activities such as searches or urgent verifications will still have to be dealt with through technical arrangements that allow the direct intervention on digital or telecommunication systems.

6. Conclusions

The study brings to the reader's attention a number of challenges the cybercrime investigator is currently facing in his domain. Ranging from the investigation phase (establishment of the competent prosecutor, acquisition of data, seizure and information exchange between jurisdictions), to the prosecutorial one (forensic examinations), such issues touch upon different legal fields, including cybercrime governance. As we have been able to demonstrate, questions arise when legal provisions are applied in concrete cases, or where interpretative dilemmas on sometimes obsolete laws (*vis-à-vis* the fast pace of modern and innovative technologies) influence the smooth performance of the investigation. More specifically, technical and governance issues complement an underlying need for more efficient implementation and interpretation of both domestic and supra-national laws on cybercrime, with a particular view to the interplay between these different normative layers. On a broader level, the Italian case study has given the opportunity to further articulate on two elements. Firstly, it demonstrates that similar questions are currently debated in other jurisdictions, as well as by the cur-

rent doctrine. Secondly, starting from the Italian analysis, we were offered the link to illustrate that a number of initiatives, both at regional and transatlantic levels, aimed at reforming the existing legal framework, may have to be calibrated to take into account technological advancements and human rights. As pointed out, in their current shape these legal novelties may present some questions, too. In particular, more reflection and a more substantive innovation of the Cybercrime Convention is needed, since its leading role could, to many extent, influence a smoother and more harmonized approach to the issues faced in both national and European Union domains. However, as the Italian and many other examples show, such claim might only solve the issue partially. More consistency with the Cybercrime Convention reform will also be needed from the opposite side, i.e. in the incorporation and implementation of new obligations into European Union and national jurisdictions, where potential interpretative and technical issues could be answered throughout reciprocal understanding on the *ratio legis* of cybercrime norms. A balanced approach, with the ultimate, unequivocally twofold goal of providing cybercrime operators with effective solutions and strong safeguards from a human rights perspective.

Note

[1]Internet World Stats, *Internet Growth Statistics*, 2017.

[2]See also S. Landau, *Listening In: Cybersecurity in an Insecure Age*, New Haven and London, Yale University Press, 2017, 221 p.

[3]See also D.S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge, Polity Press, 2014, 268 p.

[4]Council of Europe, *Convention on Cybercrime*, European Treaty Series - No. 185, 23 November 2001 (hereafter, "Convention", "Cybercrime Convention" or "Budapest Convention").

[5]Parties to the Cybercrime Convention and observer organizations.

[6]Council of Europe, *Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Convention on Cybercrime*.

[7]G. Vaciago, *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age*, Torino, Giappichelli, 2012, p. 117; A. Monti, *Rules of (Digital) Evidence and Prosecution's Actual Needs. When the Law Falls Behind Technology*, in A. Armando, R. Baldoni, R. Focardi (eds.), "Proceedings of the First Italian Conference on Cybersecurity - ITASEC17 (Venice, January 17-20, 2017)", 2017, p. 166-174.

[8]European Commission, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, COM(2018)225.

[9]Already in 2000, Belgium introduced provisions on cybercrime into its Criminal Code, more specifically provisions punishing the illegal interception (Art. 259*bis*) and unauthorized release (Art. 314*bis*) of confidential data and communication, computer forgery (Art. 210*bis*); computer fraud (Art. 504*quater*) and the hacking of computer systems (Art. 550*bis* and following). At that time, it also introduced provisions on seizure of computer data and search of computer systems in its Criminal Procedure Code. As a member of the Council of Europe, Belgium entered into the Convention on Cybercrime of 23 November 2001, following which it amended its legislation to implement the Convention. With the Act of 15 May 2006, Belgium also implemented the requirements of the Additional Protocol to the Convention on Cybercrime of 28 January 2003, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.

[10]Law No. 48/2008, 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*. For a detailed overview of the Italian framework until then, see B.J. Koops, S.W. Brenner, *Cybercrime and Jurisdiction. A Global Survey*, Information Technology & Law Series 11, The Hague, T.M.C. Asser Press, 2006, 374 p.; N. Foggetti, *Legal Analysis of a Case of Cross-border Cyber Crime*, in "The European Journal for the Informatics Professional", vol. IV, 2003, No. 6, p. 42-51.

[11]G. Vaciago, *op. cit.*; A. Monti, *op. cit.*

[12]R. Clemente, *The Pirate Bay: chiesto un risarcimento da un milione*, in "L'eco di Bergamo", 30 luglio 2009; F. Alù, *Caso "The Pirate Bay": la parola della Cassazione su file sharing e peer-to-peer*, in "Altalex.com", 11 febbraio 2010. See also Legislative Decree No. 70/2003 implementing Directive 2000/31/EU on inhibitory powers of the judiciary, derogating from the principle of free access to information society services.

[13]Cybercrime Convention, *Art. 19 – Search and seizure of stored computer data*.

[14]Corte di Cassazione, pen., 29 September 2009, No. 49437.

[15]A. Monti, *op. cit.*

[16]More specifically Art. 39*bis*, §4 Belgian Criminal Procedure Code, now Art. 39*bis*, §6 (following the amending Act of 25 December 2016).

[17]Belgian Cour de Cassation, 22 October 2013, AR P.13.0550.N/1, commented by K. Vanderhauwaert, *Het Hof van Cassatie staat de blokkering van toegang tot websites door Internet Service Providers als een vorm van databeslag toe*, in "Computerrecht", 2014/41, p. 106-111. For English commentaries, see a.o.: P. Van Eecke, A. Fierens, *In Pirate Bay Case, Belgian Supreme Court Confirms Lawfulness of Generic IP Blocking Injunctions*, in "LexGo.be", 13 January 2014; Stibbe, *Belgian Court of Cassation confirms that ISPs can be requested to block all domain names leading to a certain website*, 28 November 2013.

[18]The judgment was met with heavy criticism in the legal literature; see a.o. R. Schoefs, *Strijd tegen The Pirate Bay over andere boeg gegooid: databeslag toegestaan*, in "Tijdschrift voor Strafrecht", 2014, p. 137-138; P. Monville, M. Giacometti, *Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile?*, in "Revue du Droit des Technologies de l'Information", 2014, No. 68, p. 71.

[19]The legal localization of where a fact or event (with criminal relevance) has taken place. See also V. Fanchiotti, J.P. Pierini, *Impact of Cyberspace on Human Rights and Democracy*, in C. Czosseck, R. Ottis, K. Ziolkowski (eds.), "Proceedings of the 4th International Conference on Cyber Conflict" (CYCON 2012), Tallinn, NATO CCD COE Publications, 2012, p. 49-60.

[20]R. Wainwright, *The 'Uberisation' of International Police Work*, Linkedin, 2017.

[21]I.e., where «the action or omission that constitutes the offence has wholly or partly taken place therein, or the event

that constitutes the factual consequence of such action or omission [has happened within the Italian territory]».

[22]All translations are of the Authors, unless otherwise indicated.

[23]F. Galli, V. Mitsilegas, C. Walker, *Terrorism Investigations and Prosecutions in Comparative Law*, in "The International Journal of Human Rights", vol. 20, 2016, No. 5, p. 593-600.

[24]The principle of ubiquity states that the crime is deemed to have happened either where the harm occurred or in the perpetrator's place. Further readings at C.L. Blakesley, O. Lagodny, *Finding Harmony Amidst Disagreement Over Extradition, Jurisdiction, The Role of Human Rights, and Issues of Extraterritoriality Under International Criminal Law*, in "Vanderbilt Journal of Transnational Law", vol. 24, 1991, No. 1.

[25]H.D. Wolswijk, *Locus Delicti and Criminal Jurisdiction*, in "Netherlands International Law Review", vol. 46, 1999, No. 3, p. 361-382.

[26]G. Stessens, *Locus delicti van drughandel*, in "Rechtskundig Weekblad", 1998-99, p. 1252-1254.

[27]See also F. Verbruggen, R. Verstraeten, *Strafrecht & strafprocesrecht voor bachelors*, Antwerp, Maklu, 2013, or F. Deruyck, *Overzicht van het Belgisch strafprocesrecht*, Bruges, die Keure, 2017.

[28]H.D. Wolswijk, *op. cit.*

[29]Law No. 8/1992, 20 January 1992, *Conversione in legge, con modificazioni, del decreto legge 20 novembre 1991, n. 367, recante coordinamento delle indagini nei procedimenti per reati di criminalità organizzata.*

[30]See also A. Jamieson, *Antimafia Efforts in Italy, 1992-1997*, in "Studies in Conflict & Terrorism", vol. 21, 1998, No. 3, p. 233-260.

[31]See also L. Paoli, *Mafia and Organised Crime in Italy: The Unacknowledged Successes of Law Enforcement*, in "West European Politics", vol. 30, 2007, No. 4, p. 854-880.

[32]Monti, for instance, claims the lack of a strategic view in the Italian fight against cybercrime, in turn of pragmatic and often short-term solutions. See A. Monti, *op. cit.*

[33]See EUROPOL, *European Union Serious and Organised Crime Threat Assessment 2017*, 28 February 2017.

[34]EUROPOL, *Mastermind behind EUR 1 Billion Cyber Bank Robbery Arrested in Spain*, 26 March 2018.

[35]As Rugge (ISPI) puts it: «internet and computer crimes may be very sophisticated, and that they are particularly difficult to punish given the governance gap that characterize cyberspace», F. Rugge, *Cybercrime and International Relations*. Further reading at J. Martín Ramírez, Luis A. García-Segura, *Cyberspace: Risks and Benefits for Society, Security and Development*, Cham, Springer, 2017.

[36]Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereafter, "GDPR"); Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data (hereafter, "Police Directive").

[37]A. Mantelero, G. Vaciago, *Social Media and Big Data*, in B. Akhgar, A. Stainforth, F. Bosco (eds.), "Cyber Crime and Cyber Terrorism Investigator's Handbook", Syngress, 2014, p. 175-195.

[38]Legislative Decree No. 82/2005, 7 March 2005, *Digital Administration Code*, Art. 1(p).

[39]A. Monti, *op. cit.*

[40]Corte di Cassazione, pen., 12 June 2014, No. 24919.

[41]Such seizure typically begins under the authorization of the Court and the delegation by the public prosecutor (Art. 254 C.C.P.), or, in urgent and necessary cases, under direct initiation by the judiciary police. For the sake of this Article, electronic correspondence is deemed to be treated equally as offline post mail; further readings at G. Vaciago, *op. cit.*

[42]The C.C.P., at Art. 727, provides for the legal instruments for a letter rogatory to a foreign authority.

[43]Art. 247.1*bis* C.C.P.

[44]Unless in the cases of delayed or omitted notification, as enshrined in Art. 9 of Law No. 146/2006, 16 March 2006, on the execution and ratification of the international protocols against organized crime.

[45]Italian Constitution ("Costituzione della Repubblica Italiana"), Art. 15.

[46]I.e., when data needs to be collected and processed only for specific and previously defined purposes, without exceeding what is strictly necessary for the fulfilment of the purpose itself.

[47]See also G. Vaciago, *op. cit.*, p. 67.

[48]According to techterms.com, POP3 is «a simple, standardized method of delivering e-mail messages. A POP3 mail server receives e-mails and filters them into the appropriate user folders».

[49]An Internet Message Access Protocol (IMAP), is a standardized email protocol which enables the access to emails from a local client on a remote server. See also Techopedia.com: «The IMAP architecture enables users to send and receive emails through a remote server, without support from a particular device».

[50]Office of Legal Education Executive Office for United States Attorneys (ed.), *Prosecuting Computer Crimes*, 213 p.

[51]See, for instance, P. Van Linthout, J. Kerkhofs, *Internetrecherche: informaticatap en netwerkzoeking, licht aan het eind van de tunnel*, in "Tijdschrift voor Strafrecht", 2008, No. 2, p. 79-95; J. Kerkhofs, P. Van Linthout, *Cybercrime*, Brussels, Politeia, 2013; P. Van Linthout, *Technische en juridische aspecten van ICT criminaliteit*, in "Recht in beweging", 2010, p. 425-445; C. Conings, J.J. Oerlmans, *Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?*, in "Computerrecht", 2013/1, p. 23-28.

[52]Act of 25 December 2016.

[53]Corte di Cassazione, pen., 12 June 2014, No. 24919, cit.

[54]Indirect data (such as log files) processed by an Italian service provider are acquired by the investigator by virtue of the joined reading of Art. 256 C.C.P. (in English "Obligation to disclose and privileged secrets") and Art. 132.3 of the Legislative Decree No. 196/2003, 30 June 2003, *Codice in materia di protezione dei dati personali* (Personal Data Protection Code), as amended by the Legislative Decree No. 101/2018, 10 August 2018, implementing the General Data Protection Regulation (GDPR). The latter describes the modalities of acquisition of personal data from the service provider for criminal investigation purposes. Such a joined reading combines rules regarding the confidentiality of privileged secrets, the obligation to disclose information and the processing of personal data produced by service providers in the context of police investigations.

[55]In Italian "Sequestro Incrementale", i.e. demanding a seizure of data stored between X and Y timeframe, for then having the burden of filing a further seizure as far as the $Y+1$ to K timeframe is concerned.

[56]It is worth mentioning here, for the sake of completeness, two provisions of the Italian criminal law framework. First, Art. 727 C.C.P., titled "Transmission of rogatory letter to foreign countries", explaining the modalities under which an Italian judicial authority may seek for assistance (data handover, for example) to a foreign authority solely throughout intermediation of the Ministry of Justice or of the diplomatic

corps, unless otherwise indicated by law or in the case of urgency. Second, Art. 234*bis* C.C.P. states that any voluntary disclosure of data shall always be accepted.

[57]The European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)) recognizes the need for an acceleration in the process of exchange of electronic evidence in accordance with the GDPR and the Police Directive, acknowledging that the currently fragmented legal framework can create challenges for service providers seeking to comply with law enforcement requests, "[Calling] on the Commission to put forward a European legal framework for e-evidence".

[58]European Commission, COM(2018)225, cit.; Id., *Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, COM(2018)226.

[59]European Commission (DG Home and DG Just), *Improving Cross-border Access to Electronic Evidence in Criminal Matters – Inception Impact Assessment*, 3 August 2017.

[60]Art. 351 C.C.P., "(Acquisition of) further summary information".

[61]Unless in cases of omitted or delayed notification under Art. 9 of Law No. 146/2006, 16 March 2006, where it is allowed that some acts can be omitted or postponed due to the urgent nature of the circumstance and the severity of the crime under investigation.

[62]A. Seger, *Enhanced Cooperation on Cybercrime: A Case for a Protocol to the Cybercrime Convention*, ISPI, 2018; K. Rodriguez, D. O'Brien, M. Fernandez, *Behind the Octopus: The Hidden Race to Dismantle Global Law Enforcement Privacy Protections, Electronic Frontier Foundation*, in "Electronic Frontier Foundation", 1 August 2018; Council of Europe Cooperation against Cybercrime - Human Rights Octopus or Fishy Deals?, in "Access Now", 11 July 2018.

[63]S. Depauw, *Electronic Evidence in Criminal Matters: How About E-Evidence Instruments 2.0?*, in "European Criminal Law Review", vol. 8, 2018, No. 1, p. 62-82.

[64]See also P. De Hert, G. Boulet, *De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten*, in "Computerrecht", 2012/152, p. 324-330. For a commentary in English, see, for instance: P. De Hert, M. Kopcheva, *International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case*, in "Computer Law & Security Review", 2011, No. 3, p. 291-297.

[65]Belgian Cour de Cassation, 1 December 2015, AR P.13.2082.N, in "Tijdschrift voor Strafrecht", 2018, No. 2, p. 117, commented by J. Coppens; in "Rechtspraak Antwerpen Brussel Gent", 2016, No. 7, p. 485, commented by K. De Schepper; in "Vigiles", 2016, No. 2, p. 69, commented by R. Roex. See also N. Roland, *Court of Cassation definitively confirms Yahoo!'s obligation to cooperate with law enforcement agencies*, in "LexGo.be", 26 January 2016.

[66]Court of Appeal of Antwerp (criminal section, 12th chamber), Case 2012/CO/1054, C/1785/2013 (Yahoo! Inc), 20 November 2013, commented by G. Schoorens, *De Yahoo!-saga: verstrekking van elektronische identificatiegegevens*, in "Tijdschrift voor Strafrecht", 2014, No. 1, p. 75-76. See also F. Verbruggen, *Om af te sluiten, druk op Start': zesde rechter in Belgische Yahoozaak schaart zich achter eerste*, in "Computerrecht", 2014/3, p. 129-140; O. Leroux, *Arnaques, fraudes et escroqueries sur internet: moyens concrets d'investigation – Point sur l'affaire dite Yahoo! à la suite du second arrêt de la Cour de cassation*, in "Journal des Tribunaux", 2012, No. 40, p. 839-843; K. De Schepper, F. Verbruggen, *Belgian Substantive and Formal Criminal Jurisdiction in the Case of Prosecution of Foreign Electronic Service Providers for Failure to Cooperate. Can Alien Space Invaders Evade the Belgian Pac-Man?*, in "B-CCENTRE Legal Research Report", 2014, p. 73-99.

[67]Cf. G. Van Calster, who draws a parallel with the CJEU's Pammer/Alpenhof criteria (joined cases C-585/08 and C-144/09, Pammer and Hotel Alpenhof, ECLI:EU:C:2010:740), in his blog post *It's true! Belgian Supreme Court confirms order for Yahoo! to hand over IP-addresses*, in "GAVC Law Blog", 7 December 2015.

[68]Interestingly, the Court seemed to offer a layered approach, stating that for merely technical and assistance matters, a geographical link would suffice (for instance, the participation of the company in the nation's economy), whereas for more privacy-invasive orders (e.g., interrogatory of accused or witness), higher requirements would have to be met; cf. S. Depauw, *op. cit.*

[69]Court of Appeal of Antwerp (criminal section, 4th chamber), Case 2016/CO/1006 (Skype), commented by C. Gysels, *Hof van Beroep Antwerpen 15-11-2017, 2016/CO/1006*, in "Computerrecht", 2018/57, p. 92-102; commented by S. Royer, *Afluistermaatregel. Over de reikwijdte van medewerkingsplicht in de strafprocedure*, in "Nieuw Juridisch Weekblad", 2018, No. 375, p. 84. See also R. Chirgwin, *Belgian Court Says Skype Must Provide Interception Facilities*, in "The Register", 16 November 2017; T. D'Hulst, M. Moodley, *Belgian Court Fines Skype EUR 30,000 for Refusal to Cooperate with Data Protection Law Enforcement Authorities*, in "LexGo.be", 26 January 2017.

[70]A. Seger, *op. cit.* Further reading at: P. De Hert, C. Parlar, J. Sajfert, *The Cybercrime Convention Committee's 2017. Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted Via Soft Law*, in "Computer Law & Security Review: The International Journal of Technology Law and Practice", vol. 34, 2018, No. 2, p. 327-336.

[71]Cf. «Belgium's broad substantive criminal jurisdiction over those who fail to co-operate with Belgian law enforcement does not present an international legal problem...» in the contribution of K. De Schepper, F. Verbruggen, *op. cit.*, p. 30.

[72]G. Casal, M. Rivolta, *A National Strategy to Combat Cybercrime: A Case of Argentina*, in J. Davies, T. Janowski (eds.), "Proceedings of the 4th International Conference on Theory and Practice of Electronic Governance – ICEGOV '10" (Beijing, October 25-28, 2010), New York, ACM, 2010, p. 114-120; G.A. Arocena, *La Regulación De Los Delitos Informáticos En El Código Penal Argentino – Introducción A La Ley Nacional*, in "Boletín Mexicano de Derecho Comparado", 2012, p. 945-988; J. Clough, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation*, in "Monash University Law Review", 2014, No. 40, p. 698-736.

[73]M. Skorzewska-Amberg, *Global Threats But National Legislations. How to Adapt to the New Cyberspace Society*, in E.C. Viano (ed.), "Cybercrime, Organized Crime, and Societal Responses", 2017, Springer, p. 67-86; V. Bajovic, *Criminal Proceedings in Cyberspace: The Challenge of Digital Era*, in E.C. Viano (ed.), "Cybercrime, Organized Crime, and Societal Responses", 2017, Springer, p. 87-101; A. Kigerl, *Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates*, in "International Journal of Cyber Criminology", vol. 10, 2016, No. 2, p. 147-169.

[74]J. Daskal, *Borders and Bits*, in "Vanderbilt Law Review", 2018, No. 71, p. 185.

[75]*Ivi.*

[76]The Tallinn Manual sees the cyberspace divided in three layers: physical, network and social. It is growing opinion

that in the first two, nations are more inclined to devolve their powers in favor of multilateral forms of standards and regulations. Conversely, in the social layer (where laws regulate domains with a direct effect on the online interactions between humans, like the ones under scrutiny in this paper), governments tend to claim their sovereignty by being much more reluctant towards form of multi-party governance. See H. Yeli, *A Three-Perspective Theory of Cyber Sovereignty*, in "Prism: A Journal of the Center for Complex Operations", vol. 7, 2017, No. 2, p. 108-120. Cf. also: M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, II ed., Cambridge, Cambridge University Press, 2017.

[77] K. Rodriguez, D. O'Brien, M. Fernandez, *op. cit.*

[78] A. Tyler Ohlert, *Appealing to Reason-Able Expectations of Privacy: Increasing Appellate Review under ECPA Notes*, in "Hastings Law Journal", vol. 66, 2015, No. 6, p. 1731-1768.

[79] 18 U.S. Code, §2704.

[80] 18 U.S. Code, §2702.

[81] Aimed at both metadata and content data, only insofar as there is an actual and imminent life danger, such as death, terrorism, stalking crimes, missing children.

[82] Such legal instrument is normally compared with the Italian *Perquisizione delegata* under joined reading of Art. 247 and 250 C.C.P.

[83] Legislative Decree No. 196/2003, cit., as amended by the Legislative Decree No. 101/2018, cit.

[84] As defined by: (1) Art. 14 of the Legislative Decree No. 70/2003, 9 April 2003, transposing the "Mere Conduit Liability" principle, as enshrined in Art. 14 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'); and (2) Art. 25 of the Legislative Decree No. 259/2003, 1 August 2003 (Electronic Communication Code), which lays down the basic set of rules for the authorization of networks and services of electronic communications.

[85] In Italian *legittimo titolare*.

[86] Cybercrime Convention, Art. 32 - Trans-border access to stored computer data with consent or where publicly available: 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.

[87] Law No. 43/2015, 17 April 2015, on the Conversion of extraordinary measures for the fight against international terrorism.

[88] UN Security Council Resolution No. 2178, 2014.

[89] In terrorism studies, «[A] foreign fighter [is] an agent who (1) has joined, and operates within the confines of, an insurgency, (2) lacks citizenship of the conflict state or kinship links to its warring factions, (3) lacks affiliation to an official military organization, and (4) is unpaid.» T. Hegghammer, *The Rise of Muslim Foreign Fighters*, in "International Security", vol. 35, 2011, No. 3, p. 54-56.

[90] J. Daskal, *op. cit.*, p. 74.

[91] *Ivi*, p. 74-75.

[92] In a 2013 paper, Koops brings the attention to three examples of national implementations (Kosovo, Portugal and Romania); see B-J. Koops, *Police Investigations in Internet Open Sources: Procedural-Law Issues*, in "Computer Law & Security Review", vol. 29, 2013, No. 6, p. 654-665.

[93] *Ibidem.*

[94] *Ivi*, p. 659.

[95] *Ibidem.*

[96] *Ivi*, p. 658.

[97] E. De Busser, *Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You*, in "Groningen Journal of International Law", vol. 2, 2014, No. 2, p. 90-114.

[98] M. O'Floinn, D. Ormerod, *Social Networking Sites, RIPA and Criminal Investigations*, in "Criminal Law Review", 2011, p. 766-789.

[99] E. De Busser, *op. cit.*; Q. Eijkman, D. Weggemans, *Open Source Intelligence and Privacy Dilemmas: Is It Time to Reassess State Accountability?*, in "Security and Human Rights", vol. 23, 2013, No. 4, p. 285-296.

[100] See also F. Sampson, *Following the Breadcrumbs: Using Open Source Intelligence as Evidence in Criminal Proceedings*, in B. Akhgar, P.S. Bayerl, F. Sampson (eds.), "Open Source Intelligence Investigation, Advanced Sciences and Technologies for Security Applications", Cham, Springer, 2016, p. 295-304.

[101] E. De Busser, *op. cit.*

[102] Legislative Decree No. 82/2005, cit.

[103] I.e., a place which is accessible to anyone without limitations, regardless of the fact that the same space might belong to a private property.

[104] I.e., a place which is open to anybody whilst within the juridical availability of a subject, who can pose certain conditions on its exclusion or limitation to public access, such as a theatre or a social network like Facebook - See Corte di Cassazione, pen., 12 September 2014, No. 37596.

[105] E. De Busser, *op. cit.*

[106] I.e., the ability to exclude something or somebody to third parties.

[107] It must be noted that law enforcement officers may make unfettered use of any information that is not password-protected and accordingly, freely accessible to all web surfers, given that, as per consolidated case-law, such use does not entail the interception of private electronic or computerized communications within the meaning of Art. 266*bis* C.C.P., which, falling as they do within the personal sphere, are afforded constitutional confidentiality protection. Accordingly, law enforcement agencies are barred from accessing the profiles of social network users who choose to keep the related data confidential, since information not freely available to the public must be deemed to fall outside the scope of "open communications."

[108] Art. 4(7) GDPR. See also the Italian implementing Act: Legislative Decree No. 101/2018, cit., amending the Legislative Decree No. 196/2003, cit.

[109] B-J. Koops, *op. cit.*, p. 657.

[110] For more context, refer to the Section 3.2.3.

[111] *United States v. Microsoft Corp.*, No. 17-2, 584 U.S., 2018.

[112] See for instance, *United States v. Microsoft Corp.*, in "SCOTUS blog", 2018.

[113] *United States v. Microsoft*, in "Epic.org", 2018.

[114] U.S. Stored Communications Act (SCA, codified at 18 U.S.C. Chapter 121 §§ 2701-2712).

[115] Cross-border Access to Data: NGO Position Delivered to the Council of Europe, in "AccessNow", 18 September 2017.

[116] European Commission, COM(2018)225, cit.

[117] Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

[118] Joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

[119] P. Vogiatzoglu, *Trust Issues and the Recently Proposed EU E-Evidence Framework*, in "CITIP blog", 5 June 2018.

Further reading at: G. Robinson, *European Union. The European Commission's e-Evidence Proposal*, in "European Data Protection Law Review", vol. 4, 2018, No. 3, p. 347-352.

[120] See Section 2.

[121] *Clarifying Lawful Overseas Use of Data Act* or *CLOUD Act* (H.R. 4943).

[122] Some of which are already under discussion, for instance with regard to a bilateral agreement between the United States of America and the United Kingdom. Read more at: T. Lin, M.J.R. Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement*, Berkman Klein Center for Internet & Society, 2017, No. 7.

[123] N. Edmonds, *CLOUD Act Opens Up User Data to Foreign Governments*, in "Harvard Journal of Law & Technology", 2018.

[124] N.A. Smuha, *Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency*, in "European Criminal Law Review", vol. 8, 2018, No. 1, p. 83-115; EDRi, *EU "e-Evidence" Proposals Turn Service Providers into Judicial Authorities*, 17 April 2018; Privacy International, *Privacy International's Response to the European Commission's Public Consultation on Improving Cross-Border Access to Electronic Evidence in Criminal Matters*, 25 October 2017. See also J. Daskal, P. Swire, *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, in "Lawfare", 8 October 2019.

[125] As explained by Monti: «If this notification is not made in person because the ISP is located somewhere else in Italy, the prosecutor must send the written order to the local Police, Carabinieri or Guardia di Finanza headquarters to proceed with the formality. Otherwise the magistrate should authorize the use of any other remote communication means that guarantee the reliability of the notification. And when the order has been successfully notified, the law enforcement officers should perform, in person or with the help of a technician, all the activities necessary to extract the relevant information. An empirical finding, based on the author's professional experience of the last twenty years, shows that there are several cases where law enforcement officers try to obtain access to Internet traffic data by simple fax or regular e-mail, refusing to go back to the prosecutor to ask for a formally correct order, and delegating to the ISP the technical activities of search and consignment of the data stored in the ISP's data-centre». A. Monti, *op. cit.*

[126] Legislative Decree No. 259/2003, cit.

[127] Law No. 167/2017, 20 November 2017.

[128] Directive 2006/24/EC of the European Parliament and of the Council 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 and amending Directive 2002/58/EC.

[129] See note 117.

[130] See note 118.

[131] See for instance, Europol, *DPO Study on the data retention regime applying in the EU Member States*, in "Statewatch", 2016; also, J. Lund, *Denmark: Our data retention law is illegal, but we keep it for now*, in "EDRi blogpost", 2017.

[132] NAT techniques are IP addresses re-mapping methods.

[133] IPv4 is the fourth version of the Internet Protocol (IP).

[134] Europol, *Closing The Online Crime Attribution Gap: European Law Enforcement Tackles Carrier-Grade Nat (CGN)*, 2 February 2017. See also Hermes, *Europol's FOIA on data retention with carrier and Grade NAT*, 22 January 2018.

[135] Art. 5, Legislative Decree No. 109/2008, 30 May 2008.

[136] See note 36.

[137] See note 36.

[138] Europol, *Are you sharing the same IP address as a criminal? Law enforcement call for the end of Carrier Grade Nat (CGN) to increase accountability online*, 17 October 2017.

[139] See Art. 240 C.C. – *Confisca* ("Seizure"), Art. 260.1, 2 and 3 C.P.C. - *Apposizione dei sigilli alle cose sequestrate. Cose deperibili. Distruzione di cose sequestrate* ("Seal On Seized Goods. Perishable Goods. Destruction Of Seized Goods").

[140] MD5 is an algorithm normally used in computer sciences to produce a hash function (cryptographic function) of 128-bit value.

[141] SHA-1, which stands for Secure Hash Algorithm, is a cryptographic algorithm generating 160-bit hash value.

[142] Respectively pursuant Articles 359 and 360, 392 and seq., 220 and seq. of C.C.P. See also G. Vaciago, *op. cit.*, p. 94.

[143] For further details F. Giunchedi, *Gli accertamenti tecnici irripetibili*, Torino, UTET, 2009.

[144] See also P. Tonini, *Manuale di procedura penale*, X ed., Milano, Giuffrè, 2009.

[145] Law No. 48/2008, cit.

[146] See also Corte di Cassazione, 5 March 2009, No. 14511, where it is stated that copying computer files does not imply an unrepeatable action for the Court's admissibility assessment, provided that integrity of the evidence is preserved.

[147] G. Vaciago, *op. cit.*, p. 95.

[148] In Italian *Ignoti*.

[149] The right to self-defence is a prerogative of the indicted suspect; see also B. Reinicke, J. Cummings, H. Kleinberg, *The Right to Digital Self-Defense*, in "IEEE Security Privacy", vol. 15, 2017, No. 4, p. 68-71.

[150] Corte di Cassazione, pen., 14 July 2008, No. 33404.

[151] In the Italian Constitution, Art. 111 outlines the right to a fair trial, which implies a contradiction and the impartiality of the judicial party.

[152] Under Art. 370 C.C.P., the Judiciary Police can undertake investigative activities only with reference to those actions and examinations that can be explicitly delegated by the Judiciary Authorities.

[153] The extension of this procedural instrument to preliminary hearing followed a decision of the Constitutional Court (Corte Costituzionale, 10 March 1994, No. 77).

[154] G. Vaciago, *op. cit.*, p. 97.

[155] Noteworthy is the decision No. 1006/01 of the Court of Chieti, "almost automatically" acquitting the defendant after that the forensic analyst appointed by the prosecutors' office testified that the technical capabilities of the defendant's device were not sufficiently sophisticated to run the software that had allegedly infringed the copyrights under question in the case. For further details see A. Monti, *op. cit.*

[156] G. Vaciago, *op. cit.*, p. 96.

[157] J.C. Ortiz Pradillo, *Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain*, in "European Journal of Crime, Criminal Law and Criminal Justice", vol. 19, 2011, No. 4, p. 363-395.

[158] In Lorraine the Court emphasizes the need of an expert to collect and retain electronic evidence, in order to ensure the integrity of the data and its proper chain of custody. See also L. Kemp, *Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations)*, in "North Carolina Journal of Law & Technology", vol. 9, 2007, No. 3, p. 16-29.

[159] In *Griffin v. State* (Maryland doctrine), the Court set a high threshold for the authentication of social media evidence. According to the developed jurisprudence arising from it (*Albert Sublet IV v. State of Maryland*, No. 42, Sept. Term,

2014 and *Carlos Alberto Monge-Martinez v. State of Maryland*, No. 60, Sept. Term, 2014), such threshold underlines the necessity of peculiar features against the risk of hacking and manipulation of a profile: for instance, the password known to multiple people or the author's denial of writing a given post could be sufficient to reject the admissibility, whilst witnessed testimonies or the proven use of special software could meet such threshold. In contrast, the Texas doctrine (raised in *Tienda v. State*) established a significantly lower bar for authentication of the same type of evidence, stating that «there is no single approach to authentication that will work in all instances.» (Tienda, 358 S.W.2d at 640). See also S. Carlson, *When Is a Tweet Not an Admissible Tweet? Closing the Authentication Gap in the Federal Rules of Evidence*, in "University of Pennsylvania Law Review", vol. 164, 2014, No. 4, p. 1033-1065.

[160] F. Insa, *The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime. Results of a European Study*, in "Journal of Digital Forensic Practice", vol. 1, 2006-2007, No. 4, p. 288.

[161] EVIDENCE - European Informatics Data Exchange Framework for Courts and Evidence is an European funded project by the FP7 framework programme.

[162] EVIDENCE - European Informatics Data Exchange Framework for Courts, *Deliverable 3.1, Overview of existing legal framework in the EU Member States*, 30 October 2015.

[163] See for instance, Global Action on Cybercrime Extended (GLACY)+ project.

[164] F. Insa, *op. cit.*, p. 288.

[165] I.e., when the examination activities pertain to data, information or digital systems.

[166] In Italian *rilievo*.

[167] Corte di Cassazione, sez. 1, 9 February 1990, No. 301.

[168] Corte di Cassazione, sez. 2, 10 November 1992, No. 4523.

* * *

Le nuove sfide in tema di cyber forensics e digital intelligence: analisi critica e casi di studio in vista delle annunciate riforme legislative

Riassunto: Il saggio approfondisce alcune delle criticità emerse a livello investigativo in diverse giurisdizioni nazionali nell'applicazione delle attuali regole sulla lotta al cybercrime, evidenziando la tensione emersa tra l'apparato normativo vigente e la sua interpretazione da parte di operatori di polizia e giudiziari. La principale fonte internazionale sulla lotta al crimine informatico è la cosiddetta Convenzione sul Cybercrime del Consiglio d'Europa, firmata nel 2001 e ratificata da quasi sessanta Paesi negli ultimi diciassette anni. L'articolo analizza, in particolare, col metodo della comparazione le difficoltà interpretative osservate nell'ambito della giurisdizione italiana e di altri Paesi europei ed extra-europei. Con l'intenzione di supportare i legislatori che si accingono a novellare le norme attuali, l'articolo intende mettere in evidenza le difficoltà derivanti dalla frequente interpretazione non uniforme della Convenzione o dall'assenza di linee interpretative.

Parole chiave: Crimine informatico – Scienza forense digitale – Prova elettronica – Convenzione sul crimine informatico