DIRITTO PENALE CONTEMPORANEO

TYPES AND FEATURES OF CYBER INVESTIGATIONS IN A GLOBALIZED WORLD(*)

by Silvia Signorato

Abstract. *The article discusses the issue of cyber investigations in a general perspective, identifying the elements that go beyond a specific national legislation. Three types of cyber investigations emerge (i.e. pretrial, reactive and reactive), contributing to outline a criminal system whose preventive and proactive character tend to increase. In addition, thanks to a reversal of perspective with respect to the traditional approach of the legal doctrine, rather than concentrating on the characteristics of digital evidence, the author focuses instead on the characteristics of the investigations aimed at gathering digital evidence. In particular, the main characteristics of these investigations (i.e. technical nature, transnationality and cooperation of private entities) are discussed and the fact that they can lead to structural changes of investigation activities is pointed out. Finally, the article identifies a new major challenge in automated investigations and proposes their bipartition in order to ensure the respect for fundamental rights.*

1. Scene.

"Contemporary law, and for our purpose criminal procedure, are facing a moment of complex transition. The multiplicity of sources and their strict intertwining, their various legislative and case-law nature, their multilevel character, domestic, European, international, the hybridization between the two cultures of civil law and

* This article is a partially modified version of the text of the meeting speech at the International Biennial Conference (Section V, Criminal Sciences, Evolutions and Tendencies in Contemporary Crimininal Law), Faculty of Law of the West University of Timişoara (Romania), 28 October 2016.

(cc) BY-NC-ND 2010-2016 Diritto Penale Contemporaneo

common law they produce pose great challenges"[1]. Such a scenario is due to several contributing factors. Since the World Wide Web (hereafter simply called the Web) now permeates every aspect of life, it also influences the Criminal procedure and, therefore, is one of these factors.

The Web plays an important role as a communication platform. Nevertheless, its fundamental role is not restricted to the telecommunications industry. Nowadays, the Web is essential in management of several industrial processes, online transaction processing, transport management system and operations, health services, etc. Essential services like water supply and electricity supply rely on the Web. To give an idea of the spread and importance of the Web, it is worth remembering the fact that, at the beginning of 2016, more than 3 billion people were Internet users[2].

The contemporary world is going towards a social model where the Web gains more and more importance, leading to a Network society where, besides the people, the objects directly interact with the Web. In this regard, the term "Internet of Things" is increasingly used[3].

Moreover, it should be noted that the technological progress should lead to the development of partially or completely autonomous systems (e.g. robots[4], fully autonomous Unmanned Aerial Vehicles[5], etc.) that will be able to carry out activities that, until now, were the prerogative of human beings, including an autonomous interaction with the Web.

---

* This article is a partially modified version of the text of the meeting speech at the International Biennial Conference (Section V, Criminal Sciences, Evolutions and Tendencies in Contemporary Crimininal Law), Faculty of Law of the West University of Timişoara (Romania), 28 October 2016.

[1] R.E. KOSTORIS, *Fairness, criminal proceedings, European law. Notes of a civil law scholar* (*Lectio doctoralis* for the honorary degree), in *Journal of Eastern-European Criminal Law*, 2016, in press.

[2] See e.g. International Telecommunication Union (ITU), the United Nations specialized agency for information and communication technology (ICT), data released on 22 July 2016.

[3] For a discussion about Regulation and the Internet of Things, see INTERNATIONAL TELECOMMUNICATION UNION (ITU-D Sector), *Trends in Telecommunication Reform 2016, Report ITU*, 2016, pp. 69 ff.

[4] For discussions about robots and the corresponding legal implications, see e.g. U. PAGALLO, *The Laws of Robots, Crimes, Contracts, and Torts*, Springer, 2013; P. MORO, *Biorobotics and fundamental rights. Issues and limits of artificial intelligence*, in D. PROVOLO – S. RIONDATO – F. YENISEY (Ed.), *Genetics, Robotics, Law, Punishment*, Padova University Press, 2014, pp. 517 ff.; L. PASCULLI, *Genetics, robotics and crime prevention*, ibidem, pp. 287 ff., and S. RIONDATO, *Robotics and criminal law (robots, hybrids, chimeras and "technological animals")*, *ibidem*, pp. 589 ff.

[5] A fully autonomous Unmanned Aerial Vehicle (UAV) is not a simple drone. A drone is remotely controlled by a man. On the contrary, a fully autonomous UAV is a flying robot that is capable of carrying out a mission alone and, therefore, has some decision making abilities. This fact has significant legal implications. For example, the use of drones in the context of border surveillance is discussed by L. MARIN, *The Humanitarian Drone and the Borders: Unveiling the Rationales Underlying the Deployment of Drones in Border Surveillance*, in B. CUSTERS (Ed.), *The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspective*, Springer, 2016, pp. 115 ff., and L. MARIN – K. KRAJČÍKOVÁ, *Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights*, in A. ZAVRŠNIK (Ed.), *Drones and Unmanned Aerial Systems Legal and Social Implications for Security and Surveillance*, Springer, 2016, pp. 101 ff.

From a historical perspective, for each country the national power is at least partially based on ability to govern technological developments. Moreover, the development of technology always had repercussions on international relations. The growing importance of the Web led to a new international scenario, where the distribution of the control of Information and Communications Technology (ICT) can act on geopolitical balance. In other words, the distribution of the ICT control and the distribution of national power are strongly interlinked.

The increasing importance of the Web is a fact. However, it should be noted that the Web is neither good nor bad in itself. The specific purpose of a user can be good or bad instead. A specific act carried out by means of the Web can be legal or illegal.

A positive aspect of the Web is its enormous potential.

First of all, the Web has generated new individual rights (e.g. the right to Internet access), has led to new content of already existing rights (e.g., now the right to privacy has new contents) and constitutes a new technological modality for the exercise of the rights[6]. In particular, the Web can be a realm of freedom because it can ensure communication between citizens under a totalitarian regime as well as communication between them and the outside world. In this way, it ensures e.g. the right to freedom of expression and the right to freedom of thought, conscience and religion. Concerning the Web-related rights, it should be pointed out that Italy was one of the first world countries where an Internet Bill of Rights was developed at an institutional level[7].

Moreover, since the Web is a borderless system, it eliminates the distances in time and space. It allows an instantaneous communication between people in the most remote corners of the world and secure and fast transactions between people and/or business of different countries.

2. The use of the Web for criminal purposes.

The Web leads to new and valuable opportunities for the solution of problems facing humanity. Nevertheless, the Web can also be used for criminal purposes. In particular, some features that characterize the Web can make particularly attractive its use for criminal purposes. Therefore, it is important to discuss the reasons for this.

---

[6] According to the United Nations, General Assembly, Human Rights Council, Thirty-second session, Agenda item 3, *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, 27 June 2016 A/HRC/32/L.20 "the same rights that people have offline must also be protected online".

[7] There are several Internet Bill of Rights in the world, but they are usually due to dynamic coalition. On the contrary, the Italian Internet Bill of Rights (in Italian, *Dichiarazione dei diritti in internet*) was released on 28 July 2015 by a state institution, i.e. the Italian Parliament, Commission for rights and obligations related to the Internet (Parlamento italiano, Commissione per i diritti e i doveri relativi ad Internet).

First of all, in the absence of adequate countermeasures, the Web can be used to damage anyone from anywhere. Moreover, a person or a criminal organization can commit crimes against a lot of different people with the same effort that would be required to hit one person.

Second, techniques such as steganography or cryptography[8] can be used to ensure anonymity of an offender. For example, both techniques are implemented in the darknet, i.e. the part of the Web that is kept hidden. Under the condition that the necessary precautions are taken, anonymity is complete.

Third, the access to the Web is, in general, easy and the characterized by a very, very low cost.

For these reasons, as well as for the awareness of the difficulties in international cooperation in the field of fight against cybercrime, some criminals think that the Web is an ideal tool to commit several offences. To name a few: illegal access to a computer or a telematics system, illegal interception, computer-related forgery, computer-related fraud, offences related to child pornography, instigation to commit suicide, offences related to infringements of copyright[9].

The Web was used in the past and is currently used by every type of criminality: individuals, criminal organizations and even states. In this respect, it should be highlighted the role played by the Web in the criminal acts carried out by the so-called Islamic State. Activities such as public provocation to commit a terrorist offense, recruitment for terrorism, training for terrorism are directly carried out on the Web[10]. The self-proclaimed caliph of the Islamic State, Abu Bakr Al-Baghdadi, activated a hacking division, in view of a cyber war, a fact which is of considerable concern and requires adequate countermeasures[11].

For their part, international organizations, European Union and several states are committed in the fight against cybercrime, including the creation of centers for information security aimed at preventing the commission of different types of crimes, i.e. not only criminal acts of terror.

---

[8] See e.g. D. BUSO – D. PISTOLESI, *Le perquisizioni e i sequestri informatici*, in F. RUGGIERI – L. PICOTTI (Eds.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, 2011, p. 185, and C. MAIOLI – A. GAMMAROTA, *Steganography and steganalysis*, Racis, 2005.

[9] For discussions about cybercrime see e.g. A. KLIP, *General Report,* in *Revue international de Droit pénal*, 2014, pp. 381 ff.; U. SIEBER, *The international Handbook on Computer Crime, Computer-related Economic Crime and the Infringments of privacy,* John Wiley & Sons Inc, 1986; ID., *Computerkriminalität*, in U. SIEBER – H. SATZGER – B.V. HEINTSCHEL-HEINEGG (Eds.), *Europäisches Strafrecht,* Nomos, 2011, pp. 393 ff.; C. PECORELLA, *Il diritto penale dell'informatica,* Cedam, 2006; L. PICOTTI, *Reati informatici,* in *Enc. Giur. Treccani,* Agg., VIII, 2000.

[10] A discussion on criminal cyber investigations carried out in Italy against terrorism can be found in S. SIGNORATO, *Le misure elettroniche di contrasto al terrorismo: black list, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet,* in R. E. KOSTORIS – F. VIGANÒ (Eds.), *Il nuovo pacchetto antiterrorismo*, Giappichelli, 2015, pp. 55 ff.

[11] However, Osama Bin Laden initiated the cyber jihad a few years back. For an overall view of Cyberterrorism, see e.g. T. CHEN – L. JARVIS – S. MACDONALD (Eds.), *Cyberterrorism: Understanding, Assessment, and Response*, Springer, 2014, and S. PORTESI, *Potential Applications of Advances in Tecnology to Prevention and Response to Cases of Terrorism and Criminality: the Role of Information and Communication Technologies,* in *Cyberspazio e diritto,* 2004, n. 2, pp. 159 ff.

3. Combating cybercrime: pretrial, reactive and proactive investigations.

The amount of cybercrimes is very high. It is estimated that, worldwide, in 2015 cyber-attacks against companies led to data breach and/or loss for 700 million records, costing 400 million dollars in economic loss[12]. Beyond these attacks, there are all the attacks suffered by individuals or institutions. It should be noted that the individual cybercrime victimization rates seem to be higher in countries with lower levels of development. However, it is difficult to give a reliable estimate of the victims worldwide. This because the cybercrimes are often characterized by under-reporting and under-recording, and also because in the various legal systems there are significant differences about the possible content of the term cybercrime and of the notion itself of a victim[13].

Despite this fact, it seems that the victims of cybercrime could be divided into three categories. First of all, there are the victims who are aware of being victims of crime and who submit the corresponding report. Second, that victims who are aware of being victims of crime but, despite this fact, decide not to report, for example because the costs of the criminal trial could exceed the amount of the economic loss suffered, lack of confidence on outcome of the trial or even limited knowledge of their rights. As above stated, in the case of cybercrime the amount of missing reports from the victims is very high; no more than about 20 per cent of individual victims of cybercrime reports the crime[14]. Finally, there are the unsuspecting victims, i.e. those who are not aware that they have suffered a crime. These victims are unsuspecting either because they know the fact, but do not know that that it is a criminal offense, or because they are unaware of the offense (a typical example is an illegal access to a computer or telematics system which is not discovered by the victim).

Since there are so many cybercrime victims, an effective investigative action aimed at combating cybercrime is required. However, it is necessary to take into account the fact that the principles of appropriateness and proportionality must always

---

[12] The costs of cybercrime insurance should be added to these amounts. The state of cyber insurance is still at a less mature stage with respect to other insurance sectors. For an overview the importance of addressing cyber risk, see EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA), *Cyber Insurance: Recent Advances, Good Practices and Challenges*, 7 November 2016.

[13] With regard to the latter, see e.g. G. ILLUMINATI, *The victim as a witness*, in L. LUPÁRIA (Ed.), *Victims and Criminal Justice. European standards and national good practices*, Wolters Kluver, 2015, pp. 66 ff. For a discussion about procedural rights of the victim in the structure of the Directive 2012/29/EU, as well as in the framework Decision 2001/220/JHA see, e.g. H. BELLUTA, *Participation of the victim in criminal investigations: the right to receive information and to investigate*, in *this Magazine*, 23 December 2015.

[14] See global private sector survey cited in UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Comprehensive Study On Cybercrime*, Draft February 2013, p. xxi. The significant amount of missing reports from the victims suggests that there is the need of a comprehensive action aimed at providing information and support to the victims through free services. See e.g. L. LUPÁRIA – R. PARIZOT, *Conclusions. Which good practices in the field of victim protection?*, in L. LUPÁRIA (Ed.), *Victims and Criminal Justice. European standards and national good practices*, Wolters Kluver, 2015, p. 333.

be respected in the course of investigations, without exceptions. Such an investigative action aimed at fighting cybercrime must necessarily be implemented through cyber investigations. However, it should be noted that cyber investigations are carried out not only to combat cybercrime, but also in any case in which a digital evidence must be gathered, regardless of the specific prosecuted offence[15]. It is the case, for example, of investigations aimed at combating organized crime[16].

Nowadays, as whichever criminal offence is committed by anybody, it is increasingly necessary to gather digital evidence. This fact implies that cyber investigations are frequently carried out and, moreover, are expected to become more and more important.

This paper also highlights a particular aspect that characterize the cyber investigations, namely the fact that they are not only pretrial and reactive investigations, but they tend to become increasingly proactive ones. These kinds of investigations are now described in detail.

a) Pretrial investigations.

The pretrial investigations are carried out in order to prevent crimes from taking place. It should be noted that the criminal systems currently tend to become more and more preventive systems[17].

The cybersecurity is perceived as a critical aspect of the state security worldwide[18]. This because problems related to cybersecurity can evolve into serious threats to national or also global security, undermining the operation of national critical infrastructure and, more generally, the integrity of any computer system.

This fact has led various states to strengthen cyber defense also through specific training programs for state personnel. The authorities and bodies involved in cyber defense must face the effects of a continuous development of technology in an ever-changing world, where particularly invasive technological threats can appear. It should be noted that some regulatory acts specifically require investigators to work together with universities and public or private research centers[19]. This is because an effective preventive action can be carried out by means of both interpenetration of several bodies of knowledge and cooperation between the police and other actors, e.g. scholars.

---

[15] See the art. 14 § 2 c of the Convention on Cybercrime, which refers to "the collection of evidence in electronic form of a criminal offence", not just speaking of cybercrime offence.

[16] See e.g. I. CELINA PAȘCA, *Criminalitatea organizată în perspectiva legislațiilor europene,* Universul Juridic, 2015.

[17] See e.g. R. ORLANDI, *Attività d'intelligence e diritto penale della prevenzione,* in G. ILLUMINATI (Ed.), *Nuovi profili del segreto di Stato e dell'attività d'intelligence,* Giappichelli, 2010, p. 227 ff.

[18] V. PATANÈ, *Recent Italian Efforts to Respond to Terrorism at the Legislative Level,* in *Journal of International Criminal Justice*, 2006 (4), p. 1179, said "From the Hobbesian idea of security as a basis for power as well as for legality, we have been progressing towards a concept of security as a right standing on its own". This claim can also be referred to cybersecurity.

[19] See Directive of the President of the Italian Council of Ministers of 1 August 2015.

The pretrial investigations can be carried out either by the Security Police or the intelligence services. Cyber investigations are characterized by a continuous increase of the field of operation of the intelligence[20], which is called in this area cyber intelligence (the so-called Cybint).

It is necessary to point out that, nowadays, more and more states use spy software in pretrial investigations[21]. These systems are particularly invasive, especially in terms of privacy. In fact, they not only can capture and store any digital data contained within a computer system (computer, cloud, servers, smartphones, etc.), but also can automatically activate the webcam and microphones on the devices. In this way, they can hear everything said and film everything that happens.

The general trend of pretrial investigations is an exponential increase of the amount of collected data. The fight against terrorism has given an added impetus to this phenomenon. However, there is a serious risk that an undemocratic legislation, which could lead to new and insidious forms of totalitarianism, can also be legitimized within a democratic framework. This risk of authoritarian tendencies can only be prevented by placing clear limits to an indiscriminate collection of data and defining a clear and exhaustive list of the crimes for which the data retention is allowed[22].

It should also be noted that the size of extremely large data sets could be beyond the ability of commonly available tools to capture, manage, and process data within a tolerable elapsed time. This is the problem of "Big data", whose analysis can require supercomputers and specific analysis techniques and related research work, which are prerogatives of a limited number of states. Such an imbalance in ability in data acquisition, storing and analysis should be pointed out.

b) Reactive investigations.

Reactive investigations are carried out after a crime has been committed and the corresponding *notitia criminis* has been received by the competent authority.

A same type of cyber investigation can be regulated in a very different way worldwide. Moreover, some types of cyber investigation are governed by legislation in only certain States, while in others there is no a specific law. For example, in Italy there is not a law about the above mentioned spy software[23], which can also be used during the reactive investigations. Since the online searches cause a significant violation of the privacy of the subjects under investigation, the fact that there is not a specific law implies that the use of spy software could lead to compatibility problems with art. 8

---

[20] See THE DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA, *The Department of Defense Cyber Strategy. April 2015*.

[21] The monitoring of social media has increasing importance for government agencies.

[22] See e.g. S. SIGNORATO, *ICT, Data Retention, and Criminal Investigations of Economic Crimes*, in *Journal of Eastern-European Criminal Law*, 2015, n. 2, pp. 206 ff.

[23] The German Bundesverfassungsgericht (Federal Constitutional Court) declared in 2008 the unconstitutionality of the law of North Rhein Westfalen Land about on online searches for violation of the principles of proportionality and definiteness. Moreover, this court also recognized a new fundamental right, i.e. the constitutional right in the confidentiality and integrity of information systems (Grundrecht auf der Gewährleistung Vertraulichkeit Integrität informationstechnischer und Systeme).

ECHR (Right to respect for private and family life). This is because such an article states that "There shall be no interference by a public authority with the exercise of this right except such as is *in accordance with the law* and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

c) Proactive investigations.

The Proactive Investigations are investigations where the aspects of prevention (that characterize the pretrial investigations) and repression (that characterize the reactive investigations instead) are so strictly interconnected that it becomes difficult to see where the first aspect stops and the latter starts[24]. The proactive investigations are still relatively unknown. Until now, there has been primarily talk of proactive investigations with regard to the fight against organized crime and terrorism, pointing out that the "objective of proactive investigations is to reveal the organizational aspects of organized crime and terrorism in order to prevent its preparation or commission and to enable the establishment of reasonable ground for the initiation of a criminal investigation against the organization and/or its members"[25].

It is necessary to point out an innovative aspect that characterizes the cyber investigations; often, they tend to become proactive investigations. This fact has an important consequence because it provides a significant input towards the creation of a new criminal system where a reactive system of punishment for crimes and resocialization of offenders and a proactive system of prevention of crime and protection of public order and security are mixed. In this way, a kind of intermediate penal system is obtained. Such a change is accompanied by another phenomenon, that is an extension of the police tasks[26] and an increasingly central role of intelligence. Therefore, in some countries this process could give rise to a dangerous circumvention of the judicial guarantee[27]. It is necessary to warn against this not minor risk.

---

[24] See R.E. KOSTORIS, *Processo penale, delitto politico e "diritto penale del nemico"*, in *Rivista di diritto processuale*, 2007, pp. 4 ff.

[25] See *Resolution Eighteenth International Congress of the International Association of Penal Law, Section III: Special procedural measures and protection of human rights*[25], Istanbul, 20-27 September 2009, in *Revue international de Droit Pénal*, 2015, p. 431.

[26] See H.- U. PAEFFGEN, *Verpolizeilichung des Strafprozesses- Chimäre order Gefahr?*, in J. WOLTER, *Zur Theorie und Systematik des Strafprozeßrechts*, Hermann Luchterhand Verlag, 1995, p. 16, and D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Archivio penale*, 2016, n. 1.

[27] See R. E. KOSTORIS, *La lotta al terrorismo e alla criminalità organizzata tra speciali misure processuali e tutela dei diritti fondamentali nella risoluzione del XVIII congresso internazionale di diritto penale,* in *Rivista di diritto processuale,* 2010, p. 328.

4. Key aspects of cyber investigations.

Current literature on cyber investigations generally focuses on characteristics of a digital evidence. By contrast, in this paper focus is placed on the main characteristics of investigations aimed at gathering digital evidence. For this reason, some key aspects of cyber investigations[28] are now shown and discussed. In particular, these three aspects are considered here: technical nature, transnationality and cooperation of private entities (in particular, private companies).

4.1. Technical nature.

Cyber investigations are a kind of extremely technical investigations. Since a digital evidence is intangible, it is characterized by a significant potential instability. A digital evidence can be affected by alteration, degradation, or loss. For example, the gathering for investigative purposes of a digital image or a text file stored in a virtual space is an extremely sensitive operation because the resulting evidence can be easily altered and manipulated. An error in the acquisition process can be disastrous and the resulting evidence could be loss or unusable in a trial[29]. For this reason, it is necessary that investigations are carried out by investigators with specific technical skills.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have proposed international standards for the evidence gathering[30]. These standards concern the identification, preservation[31],

---

[28] See e.g. S. SIGNORATO, *Electronic investigations in Italian criminal proceedings,* in *Analele Universităţii de Vest din Timişoara, Seria Drept*, 1, 2014, p. 7 ss.

[29] The special nature of a digital evidence requires to rethink the current rules on evidence in the various states. This because these rules were designed with respect to material evidence. See O.S. KERR, *Digital evidence and the new criminal procedure,* in 105 *Columbia Law Review, 2005,* pp. 290 ff., and, in the Italian doctrine, e.g. M. DANIELE, *La prova digitale nel processo penale,* in *Rivista di diritto processuale,* 2011, pp. 283 ff.; G. DI PAOLO, *Prova informatica (diritto processuale penale)*, in *Enciclopedia del Diritto, Annali,* vol. VI, Milano, 2013, pp. 736 ff.; R.E. KOSTORIS, *Ricerca e formazione della prova elettronica: qualche considerazione introduttiva,* in F. RUGGIERI – L. PICOTTI (Eds.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Giappichelli, 2011, pp. 179 ff.; L. LUPÁRIA – G. ZICCARDI, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Giuffrè, 2007; L. MARAFIOTI, *Digital evidence e processo penale*, in *Cassazione penale*, 2011, pp. 4509 ff.

[30] See ISO/IEC 17020:2012, *Conformity assessment – Requirements for the operation of various types of bodies performing inspection*; ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*; ISO/IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*; ISO/IEC 27042:2015, *Information technology – Security techniques – Guidelines for the analysis and Interpretation of digital evidence*; ISO/IEC 27043:2015, *Information technology – Security techniques – Incident investigation principles and processes*; ISO/IEC 30121:2015, *Information technology – Governance of digital forensic risk framework*; ISO/IEC 27050-1:2016, *Information technology – Security techniques – Electronic discovery – Part 1: Overview and concepts*; ISO/IEC CD 27050-2: 2016, *Information technology – Security techniques – Electronic discovery – Part 2: Guidance for governance and management of electronic discovery* (Under development);

collection, processing, review, analysis, and production of electronic evidence. In particular, a careful chain of custody is strongly recommended[32]. Although the ISO/IEC recommendations are not legally binding, they are minimum common standards that should be observed by investigators all around the world, also in order to allow an effective circulation of criminal evidence between the countries.

4.2 Transnationality.

A second feature of cyber investigations is their transnationality. A digital evidence is often characterized by its dispersion across several states. For example, it can be allocated in servers located in different countries. This fact implies the need to establish global rules aimed at determining which is the State that is entitled to carry out the investigation. In this way, it can be avoided an overlap between investigations carried out by detectives belonging to different states in order to prosecute a same crime[33].

The transnationality of cyber investigations creates several issues, which are mainly due to the diversity of criminal law between countries and the difficulties of transnational investigative cooperation in criminal matters.

4.2.1. Effects of diversity of criminal law between countries.

In order to understand the issues due to diversity of criminal law between countries, an example is provided here. Suppose someone lives in Italy, for example in Rome. He uses his mobile to write a message having defamatory content and publishes it on Facebook using a fake account. If he destroys the mobile after the offence has been committed, no a copy of this defamatory message that can be directly linked to him still exists in Italy. However, a copy of the message is also stored in Facebook's database, but Facebook is an US company. In order to gather evidence, the Italian

---

ISO/IEC DIS 27050-3, *Information technology – Security techniques – Electronic discovery – Part 3: Code of Practice for electronic discovery* (Under development).

[31] About the evidence preservation, it should be pointed out that electromagnetic waves or heating can cause an alteration or erasure of data (for example, an intentional or accidental irradiation by X rays can erase the contents of some types of storage units).

[32] See E. CASEY, *Digital evidence and computer crime. Forensic science, computers and the internet*, Third Edition, Elsevier, 2011, pp. 21 ff.

[33] Regarding jurisdictional conflicts see e.g. F. CAJANI, *Interception of communications: Skype, Google, Yahoo! and Microsoft tools and electronic data retention on foreign servers: A legal perspective from a prosecutor conducting an investigation*, in *Digital Evidence and Electronic Signature Law Review*, 6, 2009, pp. 158 ff.; V. FANCHIOTTI – J.P. PIERINI, *Impact of Cyberspace on Human Rights and Democracy*, in C. CZOSSECK – R. OTTIS – K. ZIOLKOWSKI (Eds.), *2012 4th International Conference on Cyber Confl ict*. Tallin, Estonia, NATO CCD COE Publications, 2012, pp. 49-60, and UNITED NATIONS OFFICE ON DRUGS AND CRIME, *Comprehensive Study of Cybercrime, Draft – February 2013*, pp. 195 ff.

investigators could request from Facebook a copy of the message, but there is a problem. Although the Italian law, in general, punishes defamation, this action is a criminal offence only in rare cases in the USA because the protection for freedom of speech, which is covered by the First Amendment to the United States Constitution, prevails. The consequence is that Facebook could refuse to supply a copy of the defamatory message to Italians investigators, because this company could consider that the principle of double incrimination is not met. Such a principle in many countries is a pre-condition for the gathering of evidence.

This simple example highlights how effective investigative activities require not only uniformity of the crimes, but also uniformity of the facts constituting criminal offences between countries. Therefore, a harmonization of the criminal Law must be pursued on a global scale.

4.2.2. The need of international cooperation.

A second issue related to the transnationality of cyber investigations is due to the fact that, if no special agreements between states exist, ordinary forms of mutual assistance in criminal matters should be used. This means that international letters rogatory should be used. Nevertheless, the letters rogatory are characterized by long timelines. In many cases, when the letter rogatory is obtained, the data that should be acquired have been already canceled.

A significant impetus to cooperation, in particular about a faster gathering of evidence, came from the 2001 Convention on Cybercrime (cd. Convention of Budapest), which provides that: "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence" (art. 25.1). The Convention of Budapest also provides that: "Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary)" (art. 25.3).

The 2001 Budapest Convention is a Council of Europe Convention which can be signed by all countries. For this reason, it was signed by member countries and countries which are not members of the Council of Europe. At present, 55 countries signed the Convention. This is a relatively large number of countries, but is not enough[34].

It should be recalled that, at European level, on 22 May 2017 the European directive 2014/41/EU of the European Parliament and Council issued on 2 April 2014

[34] To date, it was not signed, for example, by Russia, San Marino, Argentina, Chile, Colombia, Costa Rica, Ghana, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal, and Tonga.

enters into force. This directive concerns the European Investigations Order (EIO) in criminal matters[35]. The EIO should have a horizontal scope and therefore should apply to all investigative measures aimed at gathering of any of type of evidence (except for gathering of evidence within a joint investigation team), therefore including digital evidence. Such a directive provides the more advanced regulation of transnational gathering of evidence never appeared in Europe to date[36] and replaces the letters rogatory as well as the Freezing Orders and the European Evidence Warrant. Therefore, this directive should lead to a faster European cooperation and, therefore, to a higher investigative effectiveness, also in case of cyber investigations. However, this directive will be transposed by EU member States only.

The transnational nature of the Web means that the whole world flows into it. This fact implies that universal cooperation instruments are required in order to allow a fast gathering and a preservation of the integrity of an evidence in digital form. An Eurocentric approach to the problem can no longer be used. Cooperation has to be universal because the Web is a global system[37].

4.3 Cooperation of private entities.

The third and final feature of cyber investigations concerns the role played by the cooperation between state authorities and private entities (in particular, private companies). The fact that the overwhelming majority of networks and related hardware and software systems are owned by private parties has two important consequences.

---

[35] For a discussion about *European investigation order*, see e.g. M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Processo penale e giustizia*, 2015, pp. 1 ff.; L. CAMALDO, *The European Investigation Order*, in F. RUGGIERI (Ed.), *Criminal Proceedings, Languages and the European Union*, Springer, 2014, pp. 203 ff.; M. DANIELE, *Evidence gathering in the realm of the European investigation order. From National Rules to Global Principles*, in *New Journal of European Criminal Law*, Vol. 6, Issue 2, 2015, pp. 179 ff.; ID., *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Dir. pen. cont. – Riv. trim.*, 4, 2015, pp. 86 ff.; ID., *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *this Magazine*, 28 December 2016, and T. RAFARACI, *General Considerations on the European Investigations Order*, in S. RUGGERI (Ed.), *Transnational Evidence and Multicultural Inquiries in Europe*, Springer, 2014, pp. 37 ff.

[36] See M. DANIELE, *Evidence gathering in the realm of the European investigation order. From National Rules to Global Principles*, cit., p. 180.

[37] A Technical Arrangement on Cyber Defence was concluded between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU) on 10 February 2016. The Technical Arrangement provides a framework for exchanging information and sharing best practices between emergency response teams in protecting their networks against the growing threat of cyber attacks. See also International Agreements, Council Decision (EU) 2016/2220 of 2 December 2016 on the conclusion, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences.

First of all, cooperation with private parties is necessary to ensure in advance the computer security.

Second, the cooperation with private parties is an absolute prerequisite for an effective investigation activity aimed at combating cybercrime and for gathering digital evidence for any crime.

In general, such a cooperation cannot be avoided, leading to a significant issue. The internet service providers, i.e. the organizations that provide services for accessing and using the Internet, as well as the companies that design and produce the computer systems[38] and related software packages, operate on market principles, not on criminal investigation principles. Therefore, it is possible that clashes between investigative requirements and business needs can occur, especially about the protection of customer privacy.

In this regard, the recent case of the St. Bernardino terror attack is perhaps the most emblematic example. On 2 December 2015, Rizwan Syed Farook and his wife entered into a social center for disabled. They were both ISIS-affiliated terrorists and were masked and equipped with pistols and rifles. Once inside they opened fire, killing 14 people and wounding many others, including two policemen. The investigators seized the Farook's mobile phone. They believed that this device contained very important data about further attacks. However, the phone was an iPhone 5, which is characterized by the fact that, in order to see the stored data, a code known only by the owner is required. If someone tries to type the code, and enters an incorrect code, after 10 incorrect attempts all data contained in the iPhone are destroyed. For this reason, the FBI required Apple, the iPhone manufacturer, to provide for all its phones a "backdoor" to overcome the problem related to the access code[39]. Apple refused because such a structural change could make the iPhone security worsen. Moreover, an acceptance of such a request would be a potentially dangerous precedent.

In the specific case of San Bernardino terror attack the problem was overcome by the FBI because the access code was found. Nevertheless, the basic problem remains intact. How much the right to privacy prevails? How much the investigation needs prevail instead?

There must be some firm points of references. Since privacy is a fundamental right, possibility of gathering of personal data by state authorities must be limited as much as possible. It should be permitted only in legally foreseen cases, in order to prosecute serious crimes. Otherwise, the way towards forms of mass surveillance of

---

[38] According to art. 1, *Convention on Cybercrime of Council of Europe*, 23 November 2001 computer system means "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data".

[39] Apple said "Specifically, the FBI wants us to make a new version of the iPhone operating system, circumventing several important security features, and install it on an iPhone recovered during the investigation. In the wrong hands, this software — which does not exist today — would have the potential to unlock any iPhone in someone's physical possession". See T. COOK, *A Message to Our Customers*, 16 February 2016.

population could be opened[40]. This could in turn open the way towards new and dangerous forms of totalitarianism. In the opinion of the author of this article, a state authority cannot ask a company to change the structural features of a product because, in this way, it also interferes with the freedom of economic initiative. Instead, in circumstances where structural changes are not required, since electronic data are essential elements in investigation activities, the private companies should provide the maximum collaboration to the investigators[41] in the cases provided for by law.

5. Conclusions: risks related to automated investigations.

The cyber investigations, if not properly addressed at a legislative level, could lead to a concrete risk of mass collection of data, which in turn could open the way for the return to the dark pages of history.

There is another very considerable risk, that is the risk of falling into the pitfalls related to automated surveys. Since this risk could still be not adequately perceived, it is discussed in this concluding section.

Investigators also use software packages able to autonomously carry out certain acts of investigation. Therefore, some activities of cyber investigation can be performed not by people, but directly by computers. Although these techniques are widely used in investigative practice, they seem to have rarely attracted the interest of doctrine instead.

These software packages certainly are important tools for investigators and, therefore, their use is expected to grow in the coming years. New applications (in the sense of software packages, according to the usual nomenclature) are being developed. In this paper, the fact that these applications can be divided into two different groups is proposed.

On the one hand, there are the applications aimed at taking measurements or locating. An example is the application that allows the localization on an user on Twitter[42], which can also recognize the corresponding followers and locate them. In this regard, the right of the defense to verify the performance of these applications in the specific case should be guaranteed.

---

[40] See e.g. G. DI PAOLO, *Judicial Investigations and gathering of evidence in a digital online context,* in *Revue internationale de Droit Pénal,* 2009/1, vol. 80, pp. 204 ff.; M. SIMONATO, *Young Penalists Special Report. Defence Rights and the Use of Information Tecnology in Criminal Procedure*, in *Revue international de Droit Pénal,* vol. 85, 2014, pp. 265 ff., and J.A.E. VERVAELE, *Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?,* in S. GUTWIRTH – R. LEENES – P. DE HERT (Eds.), *Reloading Data Protection. Multidisciplinary Insights and Contempary Challenges*, Springer, 2013, pp. 115 ff.

[41] A discussion on differences in legislation among the different states about the obligation of private actors to cooperate with law enforcement can be found in L. BACHMAIER WINTER, *General Report, in Revue international de Droit Pénal,*, 2014, pp. 99 ff.

[42] Twitter is an online news and social networking service.

On the other hand, there are applications that perform "quasi-human" functions and, in particular, have at least limited decision capabilities. For example, some applications are able to understand the degree of aggressiveness of a message posted on a social network by evaluating the distribution of the time spans between a word and the other. Other applications of this kind can recognize the good impulses from the bad ones and, therefore, are able to analyze the level of potential dangerousness of a subject. Some applications are based on algorithms aimed at recognizing sex, religion, age or other features of the person being monitored. Finally, there are more complex software packages that can create a profile of the suspect or suggest a subject as responsible for a particular crime.

However, there is the risk that an evidence obtained by software, without human supervision, could become a determining factor on which to base the conviction or acquittal of a subject. It is necessary to warn against this risk. In the opinion of the author, such a possibility should not be allowed and it would also be appropriate that the international conventions and laws of different states provide for the express prohibition that a decision can be based on a crucial evidence due to an automatic process of evaluation. This refusal is based on two sets of reasons.

First of all, from a technical point of view, it should be noted that, like each software, an application that performs automated surveys is not infallible. Furthermore, in certain cases, technical problems can also lead to a malfunction and, therefore, to unreliable results. If the problems were related to this point of view only, it could be enough that the defense is always able to verify the suitability of the used software.

Secondly, the use of a software for automated investigations must be evaluated from the point of view of safeguarding fundamental rights. Although an application of such a kind is calibrated in order to provide reliable output data taking into account the diversity in personal characteristic of people, it is also true that no a software package will ever be able to capture and describe all the variables that appear in humanity. The respect for human dignity requires that any conviction or acquittal must result from a close examination by human beings who are qualified to do so and, in particular, cannot be uniquely the result of the use of an algorithm, no matter how accurate, having evaluation and decision functions. The evidence provided by automated surveys having evaluation and decision functions should therefore be regarded as actual evidences if and only if they are confirmed by an human operator. An application intended for automated surveys aids the investigation activity but does not replace the investigators.

In conclusion, cyber investigations are a kind of investigations that are now absolutely necessary and whose importance is expected to significantly increase in the future. Nevertheless, major new legislative measures are necessary to ensure their effectiveness, also taking into account their transnational nature, and to safeguard respect for fundamental rights.