Turkish Journal of Computer and Mathematics Education Vol.12 No.11 (2021), 915-929

Research Article

European Conventions that make States Cooperate Against Cyber Crimes and the Problem of Electronic Evidences for Investigations and Criminal Processes

Rezarta Tahiraj[1], Sabino Porro[2]

[1]Associate Professor, Head of Scientific Research Center for Studies in Law and Economy, Economic Faculty, University of Elbasan "Aleksandër Xhuvani", Albania.
[2]Vice President, Association for Citizens Rights and Protection of the Environment, Albania. Web site: [1]Rezarta.Tahiraj@uniel.edu.al , [2]www.acrep.eu ,sabinoporro@acrep.it
Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Problem or resource. The electronic evidences are always a resource for investigations and criminal processes for the purpose of ascertaining the truth. However, when their acquisition crosses European borders, the electronic evidences, sometimes, become a problem due to difficulties of procedures that can be carried out in a third country. The issues highlighted by this article are how the European regulatory framework has evolved and how the ratification of conventions have broadened the applicability of procedures in this area, but not only, to many countries on other continents. To understand what objectively relevant results produce to the national legislation the adaptation to these conventions, the research focuses on analysis of the Italy case. In addition, this article explains how electronic evidences are now an indispensable judicial tools in the fight against the cyber crime and to counter, for example, the terrorism, the xenophobic and racist propaganda, the sexual exploitations of minors and safeguard the protection of personal data. At the end, the research is enclosed with the comparison of differences between the European investigation order, the European production order and the European conversation order of electronic evidences in the criminal matters with the purpose to reflect on the advantages that the spread of such good practices can produce for the benefit of all humanity.

Key words: Electronic Evidences, Computer Crimes, Cyber Crimes, Penal Code, Budapest Convention, European Union.

1. Introduction

The occurrence to acquire electronic evidences to be used in criminal investigations and criminal trials is a priority of judicial authorities to counter the significant increase of the cyber crimes (U.S. Department of Justice, 2001; Council of Europe, 2013; Kleijssen J. & Perri P., 2016; UNODC, 2019; Council of Europe, 2020). Very often these digital data are placed on servers and computer systems located in foreign countries and therefore become very important the collaboration between the States on the basis of an international legal framework in order to make them available when needed (Sommer P. & Brown I., 2011; Gercke M., 2012; European Court of Auditors, 2019; Jokubauskas R. & Świerczyński M., 2020).

This research analyses the main European Conventions that are producing undoubted advantages for these results but also stimulus for individual States in adapting the national legislation to the challenge of cyber crimes (Council of Europe, 2001; Csonka P., 2006; Clough J., 2015; European Union, 2015; Council of Europe, 2020) having as reference the legal model proposed by them. In particularly, it explores the modifications produced in Italy in the Penal Code and in the Criminal Procedure Code (Koops B. J. & Brenne S. W., 2006; Council of Europe, 2008; IAI, 2016)

This study also shows the main peculiarities of the Lanzarote Convention, convention for prevention of the terrorism, convention against the sexual abuse of minors, spread of racial and xenophobic hate on the internet and the requirement to harmonize these intentions with privacy, with the necessity to protect the personal data of the citizens (Fitch K., Spencer K. & Hilton Z., 2007; Council of Europe, 2007; Council of Europe, 2017; Quayle, 2020). It focuses on the peculiarities of the European Investigation Order and the procedures that must be respected by both those who emanate it than those who perform it in other State (Montero R., 2017; Kusak M., 2019).

This research provides an explanatory and comparative comparison of these legal instruments but above all offers, in addition to the elements of moderate satisfaction for the acquired knowledge of it, the awareness that the fight against cyber crimes can only be won with a broader cooperation between the States.

This paper is organized as follows: the introduction section presents the problem, the next section provides a description on the role of the Council of Europe in elaborating the conventions for the protection of the society against the cyber crimes highlighting how important is the sovranational coordination in the fight against the cyber crimes, the third section introduce the reader to the modifications produced in the Penal Code and in the Criminal Procedure Code of Italy in application of the Budapest Convention and Lanzarote Convention. The last

section of the paper is dedicated to the questions of the integration of the Budapest Convention and of the acquis communautaire against the cyber crimes which deal with the proposal of the protocols and regulations to ensure the protection of computer data. The concluding remarks provide brief assessments about the necessity to enlarge the application of the legal model outlined by the Budapest Convention to other countries in the world, reflecting on the benefits that the spread of such good practices can produce for the benefit of all humanity.

1. For a Sovranational Coordination in the Fight Against Cyber Crimes

Increasingly the crimes leave traces even in the so-called virtual world. Some crimes are even planned of committed using electronic and computer equipments. The internet crimes are growing immensely in the Internet. At the same time, the necessity of the States to adapt the response to this phenomenon increases by adopting new laws and specializing police personnel and judicial structures for the new challenge.

It is clear that however big it may be the effort of a single State it will always never be enough to face the complexity of the cases characterized, for example, by the extraterritoriality of the authors of the crimes or computer data proving the crime as well as the tools for its execution or planning.

There are two elements that, more than the others, are indispensable for combating cyber crimes: an ever wider collaboration between States, so as to become global, and the promptness of the responses that each State must provide to the requesting State useful information for prevention or repression of crimes. Think of the danger of terrorism and the exchange of information necessary to discover and stop those who plan attacks or to prevent cyber attacks on institutional national security databases. But the daily news is also made by a myriad of small and large scams for simple purchases on websites that are always crimes to be countered and from many other examples. Not least the need to protect the personal data of anyone who lawfully accesses the internet to use digital services, to protect minors from the risks of sexual exploitation, from preventing xenophobic and racist propaganda (Global Initiatives Against Transnational Organized Crime, 2019).

It can not be alone when the problems are common as well as the goals. The action of States needs not only collaboration with other States but above all supranational coordination, guidelines that make homogeneous the action to combat crimes. Two figures can provide immediately the measure of how important is the exchange of digital data between States to win the challenge against crimes: 85% of criminal investigations uses the digital data; in over 50% of cases, the criminal investigations would require requests of electronic evidence forwarded by the authority of one State to another State in the European Union. The digital data can be, in these cases, electronic evidences and their acquisition cannot be limited by national borders. If these evidences are stored on servers located abroad, national authorities must also have the ability to access it or otherwise receive it to use it in order to identify the authors of the crimes and convict them (Carrera S. & Stefan M., 2020).

1.1. The Conventions for the Protection of the Society against Cyber Crimes: the Role of the Council of Europe

An undeniable leading role has been played in the last 20 years by the Council of Europe. Fundamental is the Convention on Cyber Crimes, decided on 23 November 2001 in Budapest, which arises from the widespread awareness of the "risks that computer networks and information in electronic format can also be used to commit crimes and that the evidences related to such crimes can be stored and transferred through these networks" and has the purpose, among other things, to "make more efficient the investigation and prosecution of crimes committed in the field of computer systems and information and to consent the collection of evidences of a crime in electronic form (Council of Europe, 2001).

The Budapest Convention is expanded in its value on 28 January 2003 in Strasbourg with the Protocol on acts of racist and xenophobic nature committed by means of computer systems (Council of Europe, 2003). On 16 May 2005 was signed the Convention of the Council of Europe for the Prevention of Terrorism (Convention of Council of Europe for the prevention of the terrorism, 2005). On 25 October 2007 the Council of Europe produces the Lanzarote Convention for the protection of minors against sexual exploitation and abuse (Council of Europe, 2007). It should be noted that these three conventions have the purpose of combating crimes committed in the internet and at the same time act by grafting on the fundamental rules established with the previous Convention no. 108 of 28 January 1981 on protection of individuals with the respect to the automated processing of personal data (Council of Europe, 1981).

1.2. The Budapest Convention and the Lanzarote Convention: Global International Instruments against Cyber Crimes

It should be noted that the Budapest Convention is still the only binding international legal instrument against cyber crimes and applies exclusively to specific criminal investigations and trials. It also refers to crimes of child abuse but within the Council of Europe it was deemed to deepen better this aspect, for greater protection of the victims and to better counter the phenomenon, producing the Convention of Lanzarote.

It is undeniable that the greater risks of enticement, exploitation and abuse to the detriment of minors derive, as highlighted in the preamble of the Lanzarote Convention, also from the increased "use of communication and information technologies by minors and by the authors of crimes" and, having this phenomenon "assumed disturbing proportions on both national and international scale", "the international cooperation is essential to prevent and combat such acts".

The concept of the use of technologies for the purposes of planning and carrying out the crime against the minor is also specified in the article 23 "Solicitation of minors for sexual purposes". The parties shall take the necessary legislative measures or of another kind to make punishable the intentional proposal made by an adult, using communication and information technologies, to meet a minor under the age to that fixed in application of article 18 paragraph 2, for the purpose of committing against him a crime configured in accordance with the article 18 paragraph 1 letter (a) and article 20 paragraph 1 letter (a), if the proposal is followed by material acts that lead to such meeting".

The Convention of Lanzarote recalls in particular the recommendations of the Committee of Ministers R (91) 11 on sexual exploitation, pornography, prostitution and trafficking of children and young adults and Rec. (2001) 16 on protection of childhood from sexual exploitation, the Convention of Council of Europe on action against trafficking in human beings (STCE no. 197) as well as the Convention on Cyber Crimes (STE no. 1859). This latter (Budapest Convention), in the section dedicated to crimes relating to the contents of cyber material, explicit in article 9 the crimes of child pornography. The paragraph 1 lists the cases: a) the production of child pornography for the purpose of its spread through a computer system; b) the offer of making available the child pornography through a computer system; c) the distribution of transmission of child pornography through a computer system; d) to afford the child pornography through a computer system for oneself or others; e) the tenure of child pornography through a computer system or a computer data storage tool.

The Lanzarote Convention was absolutely necessary because, while the Budapest Convention indicates and combats crimes committed only through data and computer systems, this becomes an instrument against all forms of sexual abuse of minors, including those committed at home. It also helps to prevent the risk of this type of abuse and to train people who work in contact with children, to support victims by protecting them, for example, during judicial proceedings regarding their private life. Equally important is that it is established for these offenses that the authors are prosecuted even if the episode was committed abroad. In short, a strong deterrent even against the so-called sex tourism.

The purpose of these conventions is to stimulate the States to adopt a more adequate legislation to combat the cyber crimes through homogeneous and coordinated references. The States which have signed the Convention are 65, so it means that it has gone far beyond the countries that are part of the Council of Europe. For example, it has also been signed by Canada, Japan, United States of America and South Africa. This latter, however, did not follow up on the ratification of the Treaty but many other States that had not signed it on 23 November 2001 instead subsequently ratified and put it into force. Only three are the cases of non-ratification among the countries of the Council of Europe: Sweden, Ireland and Russian Federation. This latter has not even signed the Convention.

The Budapest Convention provides a legal basis for coordination between the States to cooperate, such as for example the exchanges of information, extradition and mutual assistance, through figures made available at any time of any day. But it is not limited to child abuse offenses. It also addresses content such as racism and xenophobia and all infringements of copyright and related rights violations, to the confidentiality, integrity and availability of data and cyber systems and infringements in the cyber field.

Think how much this Convention can help the judges and prosecutors in combating cyber crimes and how there are concretely operational tools for conducting appropriate investigations for cyber crimes through standardized procedures and international cooperation models. Not only this Convention is applied as an instrument of cooperation between the States that have ratified it but it's a legal basis, for the purposes as example of extradition of evidences or of cyber crimes authors, even with non-signatory States. In the article 29 paragraph 3 is written that "if a Party conditions the extradition to the existence of a Treaty and receives an

extradition request of another Party with which it does not have an extradition Treaty, this Convention can be considered as legal basis for extradition".

When was made reference to accessibility to data at any time of every day it was not a way of saying, but what is arranged by the article 35 of the Convention: the States must create "a contact point available 24 hours on 24 hours and 7 days on 7 days, to ensure an immediate assistance for the investigations relating to crimes referred to cyber systems and cyber data, or for the collection of evidences in electronic format of a crime". And this point of contact can be used by all those States that recognize the Convention and adhere to what is established in it.

The monitoring of Convention for the purposes of its implementation is carried out by a specific European Committee and by the Office for the Cyber Crimes Program. This latter, which has the legal office in the capital of Romania, supports the States around the world through skills-building programs. An important example is represented by Glacy project, acronym of Global Action on Cyber Crimes, which, having exhausted its temporal value from 2013 to 2016, became Glacy + to extend the experiences acquired. It supports 15 States and hub States in Africa, Asia Pacific and Latin America and the Caribbean Region – Benin, Burkina Faso, Cape Verde, Chile, Costa Rica, Dominican Republic, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Philippines, Senegal, Sri Lanka and Tonga.

What is the support action: in strengthening the capacities of States around the world to adopt laws that fight cyber crimes and to cooperate on this internationally. In summary, the objectives are three: to promote a coherent legislation, policies and strategies on cyber crimes; strengthen the capacity of law enforcement authorities to investigate cyber crimes and engage in effective police cooperation with each other and with cyber crimes units in Europe and other regions; to enable criminal justice authorities to enforce legislation and to pursue and judge cyber crimes and electronic evidences cases and engage in international cooperation.

It is almost certainly not a result that stems directly from this project, but it is equally interesting to find that more than half of the Member States of the United Nations now have a national legislation consistent with the Budapest Convention. Furthermore, in Africa there are many positive results recorded through States where cyber crimes is finally investigated and data are collected for specific criminal investigations.

1.3. The Amendments made in Italy to the Penal Code and Criminal Procedure Code in implementation of the Budapest Convention and Lanzarote Convention

The Italy which signed the Budapest Convention on the same day of its emanation and approval has proceeded to ratify the Budapest Convention on 5 June 2008. The entry into force of the Budapest Convention in Italy took place on 1 October 2008. These steps necessarily involved, precisely through the law of ratification, numerous modifications to the Italian Penal Code but also to some legislatives decrees, for example, that no. 231/2001.

The law of ratification (no. 48/2008) is composed by 4 Chapters (Gazzetta Ufficiale n. 80 del 4 Aprile 2008 - Supplemento Ordinario n. 79). The Chapter I concerns the ratification and execution of the Convention on Cyber Crimes of Council of Europe. Article 1 authorizes the President of the Republic to ratify the Convention, while the Article 2 provides its full execution starting from its entry into force, in accordance with the Article 36 of the Convention. Chapter II, composed by four articles, contains amendments to the Criminal Code and to legislative decree no. 231 of 2001 on the subject of administrative liability of legal entities. Specifically, the article 3 intervenes on crimes against the public faith referred to Book II, Title VII, of Penal Code.

The paragraph 1 modifies the article 491-bis of Penal Code which extends the case in point of forgery (material or ideological) to public or private electronic documents, defining, in the second period, such documents as "any electronic support containing data or information having evidential effectiveness or programs specifically intended to process them". In particular, the provision eliminates the second sentence of article 491-bis, which contains the definition of "electronic document". The paragraph 2 inserts a new article 495-bis in the Penal Code which sanctions with imprisonment up to one year anyone who falsely declares or certifies to the certifier the identity, status or other own conditions or those of the others.

The article 4 replaces the article 615-quinquies of the Penal Code which lays down the criminal discipline relating to the spread of the so-called computer viruses, sanctioning with imprisonment up to 2 years and with fine to 10.320 euro anyone who "disseminates, communicates or delivers a computer program by himself or by

others, having purpose or effect the damage of a computer or telematic system, of the data or programs contained therein or pertinent to it, or the interruption, total or partial, or the alteration of its functioning".

The law of ratification, while maintaining unchanged the criminal sanction (imprisonment up to 2 years and a fine up to 10.329 euro) and, essentially, without changing the definition of computer virus (which also refers not only to the damage of computer programs, but also to that of the equipments and devices), requires that the conduct is finalized to procure the author or others a profit or to bring to others damage and adds to the current conduct (dissemination, communication and delivery of the program) those of the one who procures, reproduce, import or otherwise make the program available.

The article 5 deals with the crimes against the property. In particular, the paragraph 1 replaces the article 635-bis of Penal Code, introduced by the Law no. 547 of 1993 which sanctions with imprisonment from 6 months to 3 years anyone who destroys, deteriorates or renders unusable the computer or telematic systems, programs, information or data of others. The offense is aggravated (imprisonment from 1 to 4 years) if the fact is committed with abuse of the quality of the system operator or if it occurs even just one of the aggravating circumstances of the crime of damage.

The current formulation of the case is substantially re-proposed by the ratification law of the Budapest Convention, which however omits from the incriminating offense the conduct of the person who renders, in whole or in part, useless the computer or telematic systems of others, which is now included in the article 635-quarter. Regardless of this, the only significant change concerns the prosecution of the crime which, according to the law of ratification of the Budapest Convention, occurs upon complaint of the injured person, allowing for prosecution ex officio only in the aggravated hypothesis referred to in paragraph 2. Furthermore, the paragraph 2 inserts two further articles in the Penal Code, the article 635-ter and the article 635-quarter. In both cases, starting from the case of damage of the information, data and computer programs are identified aggravated hypotheses. In particular, the article 635-ter provides the imprisonment from 1 to 5 years when the damage – as defined by the article 635-bis – concerns data or programs used by the State, by another public body or in any case of public utility (paragraph 1). In the presence of aggravating circumstances, the imprisonment is from 2 to 7 years (paragraph 2). The article 635-quarter provides the imprisonment from 1 to 5 years when the damage – as defined by the article 635-bis – or the introduction or transmission of data renders in whole or in part useless or hinders the functioning of computer systems or telematic systems of others (paragraph 1). In the presence of aggravating circumstances, the imprisonment is from 2 to 7 years (paragraph 2). The paragraph 3 inserts the article 640-quinquies into the Penal Code relating to the fraud of the electronic signature certifier. The new offense regulated therein provides the imprisonment of up to 3 years or a fine of up to 25.000 euro for the certifier who, violating the obligations set out in the digital administration code, the article 32, procures an unfair profit for himself or others with the damage of others.

Regarding the aspects of the provision somehow relevant to the areas of competence of the Finance Commission, it points out, in this context, that the article 6, which inserts a new article 25- septies into legislative decree no. 231 of 2001 on the subject of administrative liability of legal entities, which sanctions the legal person in relation to the commission of attacks on public utility systems, computer crimes and illegal data processing. In particular, there is a pecuniary penalty from 100 to 500 quotas and the prohibition from exercising the activity, the suspension or revocation of the authorizations, licenses or concessions functional to the commission of the offense, as well as the prohibition of advertising goods or services in the case of commission of the crimes of: the attack on public utility systems; the unauthorized access to a cyber or telematic system; the unlawful interception, impediment or interruption of computer or telematic communications; the installation of equipment designed to intercept, prevent or interrupt computer or telematic communications; the damage to information, data and computer programs; the damage to information, data and computer programs used by the State or by another public body or in any case of public utility; the damage to cyber or telematic systems.

On the other hand it is expected a fine of up to 300 quotas, the suspension or revocation of authorizations, licenses or functional concessions to the commission of the offense, as well as the interdiction on advertising goods or services, in the case of the commission of crimes of: illegal possession and spread of access codes to cyber or telematic systems; diffusion of equipment, devices or computer programs directed to damage or to interrupt a computer or telematic system. Finally, is excepted a pecuniary penalty of up to 400 quotas, the prohibition on contracting with the public administration, except to obtain the performance of a public service, the exclusion from concessions, loans, contributions or subsidies and the possible revocation of those already granted, as well as the prohibition of advertising goods or services, in the case of the commission of the crimes of falsification of electronic documents and digital signature certifier scam.

The article 6 repeals the second and third paragraphs of article 420 of the Criminal Code. The article 7 introduces the article 24-bis (Computer crimes and unlawful data processing) by modifying the legislative decree of 8 June 2001 no. 231 and establishing the respective pecuniary sanctions for the various cases of crimes.

The Chapter III of the ratification law of Budapest Convention makes changes to the Criminal Procedure Code and to the so-called Code of privacy, referred to in legislative decree no. 196 of 2003. In particular, the article 8 introduces certain provisions of the Criminal Procedure Code regarding the means of seeking evidence. The paragraph 1 modifies the article 244, on the subject of inspections, specifying that the judicial authority may also order findings in relation to cyber or telematic systems. The paragraph 2 intervenes on the article 247, on the subject of perquisition, by inserting a new paragraph 1-bis, concerning the carrying out of the search in an cyber of telematic system.

The condition for activating this means of searching for evidence is that there subsists a well-bounded reason to believe that data, information, programs or traces in any case pertinent to the crime are located within the computer system, even if this is protected by security measures. The paragraph 3 modifies the article 248 relating to the request for delivery of a specific thing, specifying that, in the case of preliminary inspection activities at credit institutions, the subject of the examination can be not only the acts, documents and correspondence, but also data, information and computer programs. The paragraph 4 modifies on several points the article 254, relating to the seizure of the correspondence, specifying that the items of correspondence can also be sent electronically and replaces "the post offices", to which the provision currently refers, "those who provide postal, telegraphic, telematic or telecommunication services"; the new provision also specifies that the officers of the judicial police who carry out the seizure not only cannot open the items of correspondence, but also cannot alter them. The paragraph 5 inserts a new article 254-bis in the code, which governs the methods of seizure of computer data from the cyber, telematic and telecommunications service provider. The provision provides that the judicial authority, in ordering the seizure of data, can establish that the acquisition takes place by copying on a computer support "with a procedure that ensures the conformity of the acquired data to the original ones and their immutability". The service provider must in any case take steps to properly preserve and protect the original data. The paragraph 6 modifies the first paragraph of the article 256, regarding the exhibition of documents and protection of secrecy, specifying that the seizure may concern not only the acts and documents – as currently provided for by the code – but also data and information and computer programs; therefore states that in this case the seizure can be carried out by copying the material on an adequate support. The paragraph 7 intervenes on the article 259, relating to the custody of seized thing, specifying that if the custody concerns computer data, the custodian must also be warned of the obligation to prevent their alteration or access by third parties. The paragraph 8 intervenes on the procedure for affixing seals to seized things, governed by the article 260 of the Code, specifying that, in the presence of computer data, the copies and reproductions provided for by paragraph 2 of the amended provision in the event that things subjected to seizure may be altered, must be made on suitable supports and through a procedure that ensures the conformity of the copy to the original and its immutability.

The article 9 modifies some provisions relating to the investigation activities carried out by the judicial police on their own initiatives referred to in the Book V, Title IV, of the Criminal Procedure Code. In particular, paragraph 1 inserts in the article 352, dedicated to searches, a paragraph 1-bis, which allows the officers of judicial police to proceed, still the presuppositions established to the paragraphs 1 and 2, to the perquisition of computer or telematic systems, even protected by security measures. The paragraph 2 intervenes to the article 353, relating to the acquisition of packages or correspondences, specifying, in paragraph 2, that, in an emergency case, the judicial police can receive the authorization of the public prosecutor by telephone not only for opening the package but also to the verification of the content, and that the hypotheses of suspension of the forwarding of correspondence items referred to in paragraph 3 also applies in reference to correspondence sent by computer or telematic means. The paragraph 3 adds a period to the first paragraph of article 354, on the subject of seizure and urgent investigations on places, things and people, specifying that when the assessment activity concerns information, programs of computer data, the officers of judicial police must take action so that these are not altered also providing, where possible, their duplication.

The article 10 tales the article 132 of the Code of privacy relating to the retention of data referred to telephone and electronic traffic by the service provider for the purpose of ascertaining and prosecuting the crimes inserting in this provision three new paragraphs. As regards the aspects relating to the areas of competence of the Finance Commission, it points out the new paragraph 4-ter, which assigns to the Interior Minister the power to order, also to respond to requests coming from foreign authorities, to suppliers and operators of computer or telematic services, to store and protect, for a maximum of 90 days (extendable to 6 months), data relating to electronic traffic, however excluding the contents of communications, for the purpose of carrying out the investigations aimed at the prevention of particularly serious crimes. This power can be delegated by the

Minister to the heads of central offices specialized in computer or telematic matters of the Police of State, Weapon of the Carabineri and Corps of the Finance Police. The paragraph 4-quarter provides that the supplier must comply with the request, maintaining the secret regarding the order received and the activities carried out, and recalls, in case of violation of the obligation, the sanctions envisaged for the disclosure of official secret, while the new paragraph 4-quinquies establishes that the measure adopted by the Interior Minister or its delegate must be communicated within 48 hours to the public prosecutor of the place of execution for validation, under penalty of loss of effectiveness of the measures taken.

The article 11, through an amendment to article 51 of the Criminal Procedure Code, provides, for a series of specifically listed crimes, that the functions of public prosecutor be exercised in preliminary investigations and in first instance proceedings, by the prosecutors of the Republic at the court of the capital of the district in which the competent judge has his seat. The article 12 consists of 3 paragraphs and in the first it is stated that, in the estimate of the Interior Ministry, a fund has been established with an endowment of 2 millions euro per year starting form the year 2008. In the Chapter IV are inserted the final provisions consisting of 2 articles.

The article 13 identifies the central authority required by the Convention for sending or receiving requests for extradition or provisional arrest in the Minister of Justice (paragraph 1) and delegates to the Interior Minister, in agreement with the Minister of Justice, the identification of the contact point for immediate assistance (paragraph 2). Finally, the article 14 consists of a single paragraph and indicates the entry into force of this laws on the day following its publication in the Official Journal. The law will then be published in the Official Journal General Series no. 80 of 4 April 2008 – ordinary Supplement no. 79.

This ratification law (no. 48/2008), as we have seen, was therefore not limited to introducing in Italy new types of crime into the Criminal Code but also amended the Criminal Procedure Code by establishing new provisions on the use of new technologies (example article 254-bis). It should be noted that the Budapest Convention has adopted a Protocol on acts of a racist and xenophobic nature committed by means of computer systems. This happened in 2003. The Italy signed this Protocol on 9 November 2011, so years after approving the ratification law (2008) for the Budapest Convention, but it does not escape attention that this Protocol (Treaty no. 189) had been approved and signed by the other States on 28 January 2003. If it had also been signed by Italy in 2003, the ratification law should have taken into account by extending the advantages of the Convention also to crimes related to racism and xenophobia committed using computer systems. Unfortunately this has not been the case and also it cannot be silenced that Italy has not yet ratified the additional Protocol and therefore has never made it come into force on its national territory.

Quite different from this situation is the position shown by Italy for the Lanzarote Convention which was signed on 7 November 2007 to be ratified with the Law 172/2012 entry into force on 23 October 2012 published in Official Journal no. 235 of 08.10.2012. In this case, the Italy has taken all steps to use this additional legal instrument aimed at protecting minors against sexual exploitation and abuse. The provision dictates some rules of the adaptation of internal order aimed at changing the Penal Code, Criminal Procedure Code and the penitentiary system. The changes made to the Penal Code concern the introduction of new crimes of soliciting minors, also through the Internet, and of instigation and apologia of practices of pedophilia and child pornography. Instead, the changes made in the Criminal Procedure Code concern the ritual code for crimes of district attorney competence, of the help of an expert in child psychology or psychiatry in the case of obtaining information from minors, compulsory arrest in flagrancy of the crime in the case of sexual acts with minors, of the appeal right if the acquisition of evidence with probative incident occurs with the case of solicitation of minors, of the maximum duration (two years) of the preliminary investigations in the case of commerce of juvenile pornographic material and the exclusion of plea bargain discipline for all hypothesis of child prostitution. With reference to the changes made in the penitentiary system are noticed the personal prevention measures, penitentiary benefits and free legal aid.

2. The Indispensability of the Integration of the Budapest Convention and the European Legislation against the Computer Crimes: Proposals of Protocols and Regulations to ensure the Protection of Computer Data

In the mean time, there is already a commitment at European level to prepare a second additional Protocol to the Budapest Convention. And to understand how the mentioned 3 Conventions are directly linked or dependent on compliance with the Privacy Convention, it should be noted that the European Committee for data protection is consulted on the negotiation of a second additional Protocol to the Convention of the Council of Europe on Cyber Crimes (Budapest Convention). The Committee has already highlighted the need to integrate solid data

protection guarantees into the future additional Protocol to the Budapest Convention and to ensure its consistency with the Convention no. 108 of Council of Europe, as well as with the European Union Treaties and the Charter of fundamentals rights. On the creation of a second additional Protocol to the Convention of Cyber Crimes is working since September 2017. For example, there are plans to set up joint investigation teams and joint investigations and to speed up the rapid disclosure of stored computer data in an emergency case. The goal is always the same: to provide the States with legal basis tools to standardize national laws and allow more effective cooperation in combating Cyber Crimes and protecting people and their rights in cyberspace.

2.1. The Joint Investigations Teams and the Acquisition of Electronic Evidence: Comparison Analysis of the Convention for Judicial Assistance in Criminal Matters with the Directive 2014/41/EU relating to the European Order of Criminal Investigation

In truth, this need for joint investigation teams is already provided by the Convention decided by the Council of the European Union on 29 May 2000 (Unione Europea, 2000) for judicial assistance in criminal matters between Member States. The details of the operation of these investigative teams and the modalities to order their composition and activation are described in article 13 of the mentioned Convention created in accordance with the article 34 of the Treaty of the European Union. In the paragraph 1 is written: "The competent authorities of two or more Member States may set up, by mutual agreement, a joint investigation team, for a specific purpose and a limited duration which can be extended with the agreement of all parties, to carry out criminal investigations in one or more of the Member States that make up the team. The composition of the team is indicated in the agreement".

The constitution of these teams can be done with the elements belonging to even more States. This can be understood by reading paragraph 8 of the same article: "if the joint investigation team needs the assistance of a Member State that did non participate in the constitution of the team, or of a third country, the competent authorities of the State of intervention may make a request to the competent authorities of the other State concerned in accordance with the relevant instruments of pertinent provisions".

However, the establishment of joint investigation team is held back by Directive 2014/41/EU of the European Parliament and of the Council of the European Union which, on 3 April 2014, with the introduction of the European Investigation Order (Unione Europea, 2014) decides that it should be applied to all acts of investigation aimed to obtain the existing evidence in another Member State but which is more appropriate to regulate separately the establishment of a joint investigation team and the acquisition of evidence within that team.

The article 1 of Directive 2014/41/EU established that "the European Investigation Order is a judicial decision issued or validated by a competent authority of a Member State (the "issuing State") to carry out one or more specific investigative measures in another Member State (the "executing State") for the purpose of obtaining evidence in accordance with this Directive". Contrary to what one might imagine, the European Investigation Order is not a prerogative of the investigating magistrate since it can also be requested for defense reasons and not only for accusatory purposes. In fact, in paragraph 3 of the same article it is clarified that "the issuance of an European Investigation Order may be requested by a person under investigation or by a defendant or by a lawyer acting on behalf of these latter, within the framework of the applicable rights of defense in accordance with national criminal law and national criminal procedure law".

Having established who can request the European Investigation Order remains to be clarified who can issues this provision. This can do multiple figures specified in article 2 paragraph (c) and summarized with the voice "issuing authority" and that is "a judge, a judicial body, an investigating magistrate or a competent public prosecutor in the case concerned; or any other competent authority, defined by the issuing State which, in this case, acts as an investigating authority in the criminal proceedings and is competent to order the acquisition of the evidence in accordance with national law".

When an European Investigation Order can be issued, the article 4 of the Directive: a) in relation to a criminal proceeding initiated by a judicial authority or which can be brought before it, in relation to a criminal offense under the national law of the issuing State; b) in the framework of a procedure initiated by the administrative authorities in relation to acts punishable under the national law of the issuing State as infringements of legal rules, when the decision may give rise to proceedings before a competent court, in particular, in criminal matter; c) in the context of a procedure initiated by the judicial authorities in relation to acts punishable under the national law of the issuing State as a violation of legal rules, when the decision may

give rise to proceedings before a competent court, in particular, in criminal matter; d) in connection with the proceedings referred to in letters (a), (b) and (c) relating to crimes or violations for which a legal entities can be held responsible or punished in the issuing State".

To ensure that the European Investigation Order is right, there is a sort of verification of the existence of particular conditions. It is for this that before being transmitted to the executing authority the European Investigation Order is validated, previous examination of its compliance with the conditions of issue, by a judge, a court, an investigating magistrate or a public prosecutor in the issuing State. They must verify that "a) the issue of the European Investigation Order is necessary and proportionate for the purposed of the procedure referred to the article 4, taking into account the rights of the person under investigation or accused; b) the investigation document or documents requested in the European Investigation Order could have been issued under the same conditions in a similar internal case".

The Directive 2014/41/EU relating to the European Criminal Investigation Order might make seem unnecessary the Budapest Convention of the following year. Instead, this latter is absolutely essential because it is specifically an usable tool for the so-called electronic evidence unlike the directive which is a global investigative tool. And we have already seen how the research and acquisition of electronic evidence are to be considered fundamental in carrying out the criminal investigations (so-called digital evidence).

All our daily actions in the so-called modern society are characterized by the use of electronic technology that inevitably leaves an infinite number of digital traces that in the event of crimes become electronic evidence necessary for ascertaining the facts and responsibilities. Consider, among the many digital data, to emails, audiovisual contents or instant messaging through the most widespread WhatsApp. The data are stored on a server or in cloud located in a foreign State. Many companies that manage these data have the legal office in the States that, such as for example Ireland, have not made the Budapest Convention operational and have not adhered to the directive for the European Investigation Order.

Among the operational criticalities of the Directive it should be noted that the timing is too long compared to the urgent needs of some measures, for example in cases of terrorism. The previous Convention on mutual assistance in criminal matters between countries of the European Union of 2000 (Unione Europea, 2017) establishes, for example for the interceptions, that Member States take the necessary measures to ensure that is given an answer to the request within 96 hours. But the response does not mean execution of the order. In fact, it has been established that any act of investigation is carried out with the same speed and priority as a similar internal case and within a maximum of 30 days for recognition and 90 days for execution. The awareness of this obstacle has produced, sometimes, spontaneous forms of collaboration. Investigative or preliminary material was acquired upon spontaneous delivery of the foreign server manager directly contacted by the judicial authority. But from this, as it is easy to understand, arise legal uncertainties. The electronic proof to be an evidence must be authentic and to prove that it cannot be separated, rightly, from the respect of the precise procedures for its acquisition and conversation, even when it is abroad. This has caused that less than half of the evidential requests to service providers have produced an usable result. It means that the majority of criminal cases that would require electronic evidences available abroad, even now, cannot be prosecuted efficiently.

However, to a large extent the Convention for mutual assistance in criminal matters was exceeded by the European Investigation Order Directive 22014/41/EU which concerns any act of investigation, therefore also electronic evidence but not specifically for them. The directive has the merit to establish the rules on the completion in all phases of the criminal proceedings, including the procedural one, of an act of investigation, "if necessary with the participation of the interested person for the purpose of gathering evidences". For example, in the directive it is considered that (see the point 25 of the preamble) "an European Investigation Order may be issued for the temporary transfer of that person to the issuing State or for the execution of an audition through a videoconference. However, if that person is to be transferred to another Member State for the purpose of a criminal proceedings, also to appear before a court to be processed, should be issued an European arrest warrant (EAW) in accordance with the framework decision 2002/584/GAI of the Council".

The need to guarantee always the criterion of the proportionality in reference to an arrest warrant, in this case to the European one, is contained in point 26 of the preamble of the Directive which delegates this task to the issuing authority: "to guarantee a proportionate use of the EAW, the issuing authority should examine whether an European Investigation Order constitutes an effective and proportionate means of carrying out criminal proceedings. The issuing authority should examine, in particular, whether the issue of an European Investigation

Order for the purpose of an audition of a person subjected to investigation or of a defendant through the videoconference could be an effective alternative".

The European Investigation Order has the merit to establish an unique regime for the acquisition of the evidences. For certain types of investigative acts, such as the temporary transfer of detainees, the audition through the videoconference or teleconference, the acquisition of the information on bank accounts or banking transactions, the deliveries controlled or the operations of the infiltration, "however, are necessary the additional provisions which should be provided by the European Investigation Order". The investigative acts which involve the acquisition of the evidence in real time, continuously and for a specified time should be the subject of the European Investigation Order, but they should be agreed between the issuing State and the executing States, where necessary, practical arrangements to reconcile the existing differences between the national laws of these States" (point 24 of the preamble of Directive). Finally a curiosity: but who pays the costs? The answer: the costs of executing the European Investigation Order are supported by the State in which it is executed. Read the article 21 paragraph 1: "the executing State supports all the costs incurred in the territory of the executing State related to the execution of an European Investigation Order".

2.2. The Electronic Evidence: Judicial Instruments in the Fight against Cyber Crimes

A further important step forward is taken four years later. In fact, in the year 2018, the European Parliament and the Council of the European Union drew up a proposal for a Regulation on European orders for the production and storage of electronic evidence in criminal matters. The proposed Regulation established that the European orders are binding, both for the production and for the preservation of electronic evidence. The orders, for both cases, are issued or validated by a judicial authority of a Member State and can be notified to the service providers of electronic communications, social networks, online marketplaces, other hosting service providers and internet infrastructure providers such as IP address and domain name registers, or their legal representatives, if any.

The proposed Regulation also establishes that the orders for the production of data relating to subscribers or accesses can be issued for any crime, while those for the production of data relating to operations or content can be issued only for crimes punishable in the issuing State with a prison sentence of a duration at least 3 years or for specific crimes specified in the proposal and if there is a specific link with electronic tools and crimes falling within the scope of Directive (EU) 2017/541 on the fight against terrorism (Unione Europea, 2017).

The Regulation proposed by the European Parliament and the Council of Europe is thought not to replace the European Investigation Order but to provide the authorities with an additional tool, for example, for the electronic evidence. In fact, introducing the European Production Order and the European Conservation Order, the proposed Regulation makes easier, in the context of criminal proceedings, to secure and collect electronic evidences stored or held by service providers in another jurisdiction. The article 2 of the proposed Regulation clarifies what is meant by the "European Production Order": the binding decision of an issuing authority of a Member State that orders a service provider which offers services in the European Union and is established or represented in another Member State to produce the electronic evidences. Also, clear is "European Conservation Order": the binding decision of an issuing authority of a Member State which enjoins to a service provider who offers services in the European Union and is established or represented in another Member State to preserve the electronic tests in view of a subsequent request of production.

Then there is a further distinction between these two regulatory instruments. The European Production Order have the purpose of obtaining evidence through access to transactions and contents. This is an invasive tool and for this it has been established that need the validation of a judge. The European Conservation Order, on the other hand, are considered less invasive than European Production Order and therefore can be requested by a prosecutor without the need for validation by a judge. The European Conservation Order have a less intrusive perceptive content on the computer freedom of the data owner. There is also another important difference to be noted: European Production Order and the European Conservation Order, contrary to the provisions of the European Investigation Order, cannot be requested by the defendant's defense nor by the injured person. Furthermore, the proposed Regulation clarifies how the new tools (European Production Order and European Conservation Order) may only be valid for requesting the delivery or storage of existing electronic evidence and not for the interception in real time of computer data, as this activity must be requested through the pre-exiting forms of judicial cooperation including the European Investigation Order. No procedural acts are sent to ask the European Production Order and the European Conservation Order but only information aimed at clarifying what you want to achieve. In this regard, it is specified that the European Production Order or the European

Conservation Order is sent to the service provider through an European Production Order Certificate or a certificate of European Conservation Order (European Conservation Order Certificate). These certificates contain the same mandatory information as shown in the European Investigation Order, except the reasons of the necessity and proportionality of the measure or other details on the case. It should also be clarified that the two new instruments can only be used in the course of a criminal proceeding that has already begun and this provision assumes a fundamental character for the purpose of interpreting of the correct range of action of the new rules, which can never be used to establish a state legitimacy to require forms of collaboration from individuals aimed at providing evidence in relation to a preventive monitoring activity of any illegal activities that have not found a preliminary consecration in a provision for registration in the register of the type referred to in the article 322 of the Criminal Procedure Code; in fact, it is from that moment that the rights of defense assume their autonomy, such as to justify the procedural guarantees provided by the Commission. Then operational differences are also found in the applicability of the European Production Order. For example, the European Production Order for the production of the data relating to the subscribers or data relating to accesses can be issued for any crime. The European Production Order for the production of related data to the operations or related data of content can only be issued for offenses punishable in the issuing State with an imprisonment punishment of a maximum duration at least 3 years, or for the following offenses, if committed in whole or in part by means of an information system; the offenses referred to in the articles 3, 4 and 5 of the framework decision 2001/413/GAI of the Council (Unione Europea, 2001); the offenses referred to in the articles from 3 to 7 of the Directive 2011/92/EU of the European Parliament and Council of Europe (Unione Europea, 2011); the offenses referred to the articles from 3 to 8 of the Directive 2013/40/EU of the European Parliament and of the Council of Europe (Unione Europea, 2017); for the offenses referred to the articles from 3 to 12 and of the article 14 of the Directive (EU) 2017/541 of the European Parliament and of the Council of Europe.

The proposed Regulation starts from the observation that "in some situations the European Investigation Order is preferable for public authorities, for example, when several investigative acts must be carried out in the executing Member Sate" and then come to affirm that "obtaining of electronic evidence presents specific problems that do not concern the other investigative acts contemplated by the Directive of the European Investigation Order "and therefore" instead of modifying the Directive of the European Investigation Order, it was decided to create a new tool for such tests", that is precisely the proposed Regulation.

But one has to wonders how many and to what extent are the States ready to use electronic evidence. In many courtrooms in Italy, digital documents are exhibited only after they have been transferred to material supports, thus becoming, for example, paper. There are also judgments that even, as in the case of the Court of Naples (15 July 2013, no. 10812), judge electronic evidence inadmissible or illegitimate for the sole fact, absurdly, of not having a material nature. In other countries, however, such as Sweden, the procedural documentation is all in electronic format and the dossier containing the evidence is sent electronically to the courts. The Sweden, it should be added, paradoxically never made the Budapest Convention operation even though it was one of the first to sign it on 23 November 2001.

It is considered important to point out, for the completeness of the information, the Regulation (EU) 2018/1727 of the European Parliament and Council of Europe of 14 November 2018 which establishes the Agency of the European Union for the criminal judicial cooperation Eurojust (Unione Europea, 2018) and substitutes and abolishes the Decision 2002/187/GAI of the Council of Europe. Eurojust has been established in the year 2002 as an European Union body with legal personality with the aim to stimulate and improve the coordination and cooperation between the competent judicial authorities of the Member States, in particular, in relation to serious forms of organized crime. The new Regulation was decided because there were so many changes to be made according to the purpose of enhancing the operation of the structure that it was decided, for clarity, to repeal the previous regulation and put another one into effect.

The panorama of the Conventions, Directives and Regulations continues with the Regulation of the 17.4.2019 relating to Enisa (Agency of the European Union for the Cyber Security) and the certification of the cyber security for the technologies of the information and communication (Unione Europea, 2019). The Regulation, this latter which abolished the previous Regulation no. 526/20143 on the cyber security (European Union, 2013) which abolished the Regulation (EU) no. 460/2004 (Unione Europea, 2004). Enisa has the task to favor a closer collaboration with the universities and research institutes with the aim to reduce the dependence of cyber security products and services from non-European countries. This is because, as written in point 5 of the considerations contained in the text of the Regulation "cyber attacks are on the rise and the greater vulnerability to threats and cyber attacks of a connected economy and society requires a strengthening of the defenses". This could mean that the fears are such as to create a sort of barrier, also relying on the awareness of the citizens, to the imports of

non-European technology but this does not prevent the search for closer forms of collaboration, for example, on the production and storage of evidence digital in non – European Union countries.

Indeed, on 6 June 2019, two months after the Enisa Regulation, the Council of the European Union authorized the European Commission to negotiate an agreement with the United States of America aimed to facilitate the access to the electronic evidence to be used in investigations and judicial proceedings of criminal procedure. It should be clarified that the European authorities already see the positive collaboration, on a voluntary basis, of service providers established in the United States of America in providing electronic evidence. The agreement that is to be achieved with the United States of America would, however, also create direct cooperation with service providers. This small detail would greatly reduce the times, shortening the deadline for the transmission of the requested data to 10 days, which is currently about 10 months.

The same proposal to be able to go directly to service providers or to their legal representatives to acquire electronic evidence useful in criminal proceedings has become operational between requesting authorities and recipients subjects in the European Union countries. But who are the legal representatives? On 8 March 2019 the Council defines the rules for their appointment. Their role is to receive and respond to orders for the acquisition and retention of electronic evidence. In this the figure of legal representatives is very important in view of the lack of a general legal obligation for the non European Union service providers to be physically present in the Union when they provide you with services. The Council has established, moreover, that service providers and legal representatives can be held jointly and severally liable in the event of non-compliance and also can also be used for the acquisition of types of evidence other than electronic evidence and to receive other law enforcement requests, such as European Investigation Order, without prejudice to specific procedures provided for other legal instruments fur judicial cooperation in criminal proceedings. This of the rules for the appointment of legal representatives is a further important step forward that concretely demonstrates the willingness of the States to strengthen the commitment to make the fight against computer crimes ever more specific and profitable.

3. Discussions and Conclusions

The States have no alternatives to the cooperation between them if they want to be successful in the daily challenge that the crime makes in using technology and information systems. This latter are rapidly evolving and the internet connections place and move, produce and delete digital data anywhere in the world extremely quickly. Some of this data is electronic evidence of crime and its retention and acquisition is essential for criminal investigations and criminal trials.

Each State must have the possibility of being able to seize electronic evidence of crimes even if they are located on the serves in another country. To do this, concrete collaboration is required between States that must legislate in order to adapt the current legislation to the need to foresee and combat computer crimes as well. Even this effort, although commendable, would be ineffective if it were not accompanied by a reference model, by an international legal instrument.

The Council of the European Union and the European Commission have produced the Budapest Convention which is currently the strongest legal instrument of reference in the world for combating computer crimes. It is interesting to note how this Convention is strengthened and interacts with the existence of other Conventions approved in the European context and extended to the participation of other countries in the world, for example, the Lanzarote Convention, that for the Privacy, the prevention of terrorism and the Protocol for the fight against racism and xenophobia.

To understand what objectively relevant results produces to the national legislation the adaptation to these Conventions it is sufficient to examine, as was done in this study, the case of Italy. Limiting the analysis to the Budapest Convention it is noted that not only the Criminal Code but also the Criminal Procedure Code have been modified making consequently defined the cyber crime and also the methods to acquire and use the electronic evidence. Think how many criminal offenses are committed on the Internet every day. Think of copyright violations, computer fraud, child pornography and network security violations.

The Budapest Convention indicates how to combat these crimes. The road is drawn. We are considering the creation of a second additional protocol to the Convention and this means that we remain on the right path. Now, however, it is necessary to continue on the same path without delay, extending the application of this legal model as much as possible to other countries in the world. This study is intended to be a contribution to reflecting on the benefits that the spread of such good practices can produce for the benefit of all humanity.

References

1. U.S. Department of Justice (2001). Electronic Crimes Needs Assessment for State and Local Law Enforcement. Research Report of National Institute of Justice. Retrieved from: https://www.ncjrs.gov/pdffiles1/nij/186276.pdf.
2. Council of Europe (2013). Strategic Priorities for the Cooperation against Cyber Crimes in the Eastern Partnership Region. Data Protection and Cybercrime Division, Kyiv-Ukraine. Retrieved from: https://rm.coe.int/1680300ad4.
3. Kleijssen J. & Perri P. (2016). Cybercrime, Evidence and Territoriality: Issues and Options in Netherlands Yearbook of International Law: the changing nature of territoriality and international law, pages 147-173. Retrieved from: https://rm.coe.int/cybercrime-evidence-and-territoriality-issues-and-options/168077fa98.
4. UNODC (2019). Report on the Meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 27 to 29 March 2019. UNODC /CCPCJ/EG.4/2019/2. Retrieved from: https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March 2019/Report/UNODC_CCPCJ_E.
5. Council of Europe (2020). The Budapest Convention on Cybercrime: benefits and impact in practice. Cybercrime Convention Committee (T-CY), T-CY(2020)16, 13 July 2020. Retrieved from: https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.
6. Sommer P. & Brown I. (2011). Reducing Systemic Cybersecurity Risk in OECD/IFP Project on Future Global Shocks, IFP/WKP/FGS(2011)3, 14 January 2011. Retrieved from: https://www.oecd.org/gov/risk/46889922.pdf
7. Gercke M. (2012). Understanding cybercrime: phnenomena, challenges and legal response. Infrastructure Enabling Environment and E-Application Department, ITU Telecomunication Development Bureau Publication. September 2012. Retrieved from: http://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=AroundWeb
8. European Court of Auditors (2019). Challenges to effective EU cybersecurity policy. Briefing paper. March 2019. Retrieved from: https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416
9. Jokubauskas R. & Świerczyński M. (2020). Is revision of the Council of Europe guidelines on electronic evidence already needed? Utrecht Law Review, 16(1), pages 13–20. Retrieved from: http://doi.org/10.36633/ulr.525.
10. Council of Europe (2001). Convention on Cybercrime. Details of Treaty ETS no. 185. Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
11. Csonka P. (2006). The Council of Europe's convention on cyber-crime and other European initiatives in Revue internationale de droit pénal 2006/3-4 (Vol. 77), pages 473 à 501. Retrieved from: https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm
12. Clough J. (2015). Principles of cybercrime. Second edition, Cambridge University Press, October 2015. Retrieved from: https://www.cambridge.org/core/books/principles-of cybercrime/F172001ECA8742B5C3E0678CDF977718.
13. European Union (2015). The law enforcement challenges of cybercrime: are we really playing chatch-up? Study for the LIBE Committee, European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, Brussels 2015. Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf.
14. Koops B. J. & Brenne S. W. (2006). Cybercrime and jurisdiction: A global survey, in Information Technology & Law Series, TMC Asser Press, The Hague 2006, pages 227-239. Retrieved from: https://core.ac.uk/download/pdf/187790105.pdf
15. Council of Europe (2008). Profiles on Counter-Terrorist Capacity: Italy. Committee of Experts on Terrorism (CODexter). November 2008. Retrieved from: https://www.legislationline.org/download/id/3131/file/CODEXTER%20Profile%202008%20ITALY.pdf.
16. IAI Istituto Affari Internazionali (2016). EUnited against crime: improving criminal justice in European Union Cyberspace. Documenti IAI 16/17. November 2016. Retrieved from: https://www.iai.it/sites/default/files/iai1617.pdf.
17. Fitch K., Spencer K. & Hilton Z. (2007). Protecting children from sexual abuse in Europe: safer recruitment of workers in a border – free Europe in NSPCC Inform. November 2007. Retrieved

from:https://childhub.org/en/system/tdf/library/attachments/696_708_EN_original.pdf?file=1&type=node&id=6936

18. Council of Europe (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Treaty of Series no. 201. Lanzarote 25.10.2007. Retrieved from: https://rm.coe.int/1680084822.
19. Council of Europe (2017). 2nd Implementation Report on Protection of children against sexual abuse in the circle of trust: the Strategies. Lanzarote Committee of the Parties to the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse. Council of Europe, T-ES (2017)12_en_final. Retrieved from: https://rm.coe.int/t-es-2017-12-en-final-lanzarotecommitteereportcircleoftruststrategies/16807b8959.
20. Quayle E. (2020). Prevention, disruption and deterrence of online child sexual exploitation and abuse. ERA Forum 21, 429–447 (2020). Retrieved from: https://doi.org/10.1007/s12027-020-00625-7
21. Montero R. (2017). The European Investigation Order and the Respect for Fundamental Rights in Criminal Investigations, Eucrim – European Criminal Law Association Forum, 2017/1, pages 45-50. Retrieved from: https://doi.org/10.30709/eucrim-2017-006.
22. Kusak M. (2017). Mutual Admissibility of Evidence and the European Investigation Order: aspirations lost in reality. ERA Forum 19, 391–400 (2019). Retrived from: https://doi.org/10.1007/s12027-018-0537-0.
23. Global Initiatives Against Transnational Organized Crime (2019). Annual Report 2019. Retrieved from: https://globalinitiative.net/wp-content/uploads/2020/07/GI-TOC-Annual-Report-2019.pdf.
24. Carrera S. & Stefan M. (2020). Access to electronic data for criminal investigations purposes in EU, CEPS Paper in Liberty and Security in Europe, No. 2020-01, February 2020. Retrieved from: file:///C:/Documents%20and%20Settings/Rezarta%20%20Tahiraj/Documenti/Downloads/LSE20120-01_JUD-IT_Electronic-Data-for-Criminal-Investigations-Purposes.pdf.
25. Consiglio di Europa (2005). Convenzione del Consiglio d'Europa sulla criminalità informatica STE n°185-23/11/2001. Retrieved from: https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185
26. Council of Europe (2003). Additional Protocol to the Convention on Cyber Crime, relating to the criminalization of acts of a racist and xenophobic nature committed by means of computer systems STE n°189-28/1/2003. Retrieved from: https://www.coe.int/it/web/conventions/search-on-treaties/-/conventions/treaty/189.
27. Council of Europe (2005). Convention of Council of Europe for the prevention of the terrorism, 2005. Details of Treaty No.196 Convention on the Prevention of Terrorism. Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/196.
28. Consiglio di Europa (2007). Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e gli abusi sessuali STCE n°201-25/10/2007. Retrieved from: https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/201.
29. Council of Europe (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, Strasbourg, 28.I.1981. Retrieved from: https://rm.coe.int/1680078b37.
30. Gazzetta Ufficiale n. 80 – Supplemento ordinario n. 79 (2008). Legge 18 marzo 2008, n. 48 "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". Retrieved from: http://www.parlamento.it/parlam/leggi/08048l.htm.
31. Unione Europea (2000). Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati Membri dell'Unione Europea C197/01-29.5.2000. Gazzetta Ufficiale 197/2000. Retrieved from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:197:0001:0023:IT:PDF.
32. Unione Europea (2014). Direttiva (UE) 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale L.130/1-03.04.2014. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014L0041&from=HU.
33. Unione Europea (2017). Direttiva (UE) 2017/541 del Parlamento Europeo e del Consiglio sulla lotta contro il terrorismo, L.88/6-15.03.2017. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017L0541&from=IT.
34. Unione Europea (2017). Direttiva (UE) 2017/541 del Parlamento Europeo e del Consiglio sulla lotta contro il terrorismo, L.88/6-15.03.2017. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017L0541&from=IT.
35. Unione Europea (2001). Decisione quadro 2001/413/GAI del Consiglio, del 28 maggio 2001, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

Gazzetta Ufficiale Unione Europea L 149/2.6.2001. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:l24212.

36. Unione Europea (2011).Direttiva 2011/92/UE del Parlamento Europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile e che sostituisce la decisione quadro 2004/68/GAI del Consiglio. Gazzetta Ufficiale Unione Europea L.335/17.12.2011. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32011L0093&from=IT.
37. Unione Europea (2017). Direttiva (UE) 2017/541 del Parlamento Europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio. Gazzetta Ufficiale Unione Europea L.88/31.3.2017. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32017L0541&from=IT.
38. Unione Europea (2018). Regolamento (UE) 2018/1727 del Parlamento Europeo e del Consiglio del 14 novembre 2018 che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio. Gazzetta Ufficiale Unione Europea L.295/138/21-11-2018. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1727&qid=1608807785501&from=IT.
39. Unione Europea (2019). Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»). Gazzetta Ufficiale Unione Europea L151/15/7.6.2019. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=EN.
40. Unione Europea (2013). Regolamento (UE) n. 526/2013 del Parlamento Europeo e del Consiglio del 21 maggio 2013 relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004. Gazzetta Ufficiale L.165/41/18.6.2013. Retrieved from: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32013R0526&from=EN.
41. European Union (2004). Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (2004) OJ L 77/13.3.2004. Retrieved from: https://eur-lex.europa.eu/eli/reg/2004/460/2013-06-19/eng/pdfa1a.