Electronic investigations in Italian criminal proceedings

Dr. Silvia SIGNORATO[*]
University of Padua
Faculty of Law

Abstract

This article is aimed at providing a general overview on electronic criminal investigations in Italy. At first, the concept of electronic criminal investigations is defined, then the peculiarities of such investigations are analysed. Next, the Italian Code of Criminal Procedure, which contains the procedural guidelines for these investigations, is examined and its main problematic aspects are pointed out and discussed.

Keywords: *Italy, criminal trials, criminal proceedings, electronic criminal investigations, electronic evidence, computercrime and cybercrime*

Rezumat

Articolul oferă un cadru general privind cercetarea penală a infracțiunilor informatice în Italia. În acest scop este definit, în principal, conceptul de cercetare penală informatică. În al doilea rând, vor fi analizate particularitățile cercetării penale ale infracțiunilor informatice. Un alt aspect vizează analiza dispozițiilor din Codul de procedură penală italian care reglementează această materie. În final, vor fi subliniate aspectele problematice ale acestei materii.

Cuvinte-cheie: *Italia, proces penal, cercetare penală, cercetare penală informatică, probe informatice, infracțiuni informatice și cibernetice*

1. Introduction

Globally, information technology has permeated nearly every aspect of reality. Hence, it was all but inevitable that the effects of this same technology would be felt by the Italian criminal system. Its effects are felt, on one hand, in the area of criminal law; on the other hand, they are felt at the level of criminal trial and also, as this article seeks to show, in relation to criminal investigations.

[*] silvia.signorato@unipd.it

a) *At the level of criminal law*, the Italian system has been forced to reconsider already existing crimes and to define new ones. Information technology has made possible an array of so-called computer crime, or in those cases involving the Internet, cybercrime[1]. Computer crime and cybercrime represent, in reality, a macro-category which can be divided into two groups.

On one hand, there are those "uncommon crimes" which are normally committed by means of computer technology (as in crimes involving illegal access to a telematics or computer system). Such crimes are termed computer crimes or cybercrimes in the purest sense.

On the other hand, "common crimes" can be committed even without the use of information technology. They are crimes for which the computer represents only a possible means by which to carry out the crime (as in the instigation to suicide). Such crimes are termed computer crime or cybercrime in a broader sense.

b) *At the level of criminal investigations*[2], there is a growing use of information technology within the field of investigation itself. In fact, investigators make use of information technology for two main reasons.

First of all, clearly, they must do so in the case of investigations centered on computer crime or cybercrime in the strictest sense of these terms, as well as in their broader sense.

Secondly, they may do so while investigating crimes committed without the use of information technology. An example is the relevance for investigation

[1] As regards computer crimes, see U. SIEBER, *La délinquance informatique* (French translation by S. Schaff and M. Briat of *The international Handbook on Computer Crime, Computer-related Economic Crime and the Infringements of Privacy*, 1986), Story-Scientia, 1990; U. SIEBER, *The international Emergence of Criminal Information Law,* vol. 1, Carl Heymanns Verlag KG, 1992, vol. 1; U. SIEBER, *Computerkriminalität,* in U. Sieber, F.-H. Brüner, H. Satzger, B.v. Heintschel-Heinegg (Hrsg.), *Europäisches Strafrecht*, Nomos, 2011, 393-421. In Italian legal doctrine, see L. PICOTTI, *Reati informatici,* in *Enc. giur. Treccani,* Agg., VIII, Roma, 2000; C. PECORELLA, *Il diritto penale dell'informatica*, Cedam, 2006; C.S.S. IPPOLITO, *Informatica, internet e diritto penale,* III ed., Giuffrè, 2010.

[2] Italian law distinguishes between preventive (indagini preventive) and preliminary investigations (indagini preliminari). a) Preventive investigations are geared towards the prevention of the execution of a crime. For example, there is a provision for preventive wiretapping (Article 226 of Norme di attuazione, di coordinamento e transitorie of the Italian Code of Criminal Procedure). In Italy, such wiretapping is not generally permitted, except to prevent serious crimes. b) On the other hand, preliminary investigations (the subject of this article), are carried out only after the registration of offence notice (notizia di reato) in the appropriate register. Preliminary investigations, moreover, must be carried out within a peremptory time period determined by legislators. Possible evidences provided by investigations carried out beyond such time limits cannot be used in a trial. Regarding the characteristics of preliminary investigations in Italy, see F. CAPRIOLI, *Indagini preliminari e udienza preliminare,* in G. Conso, V. Grevi, M. Bargis (eds.), *Compendio di procedura penale,* VI ed., Cedam, 2012, 493-662.

purposes of a video tape containing images of a homicide in progress. Another example is the case of data provided by a drone in the event of a kidnapping.

The importance of giving special consideration to electronic investigations is due to the increasing incidence of such investigations in the nature of investigative work itself, combined with their peculiarities.

In the Italian legal system, however, there does not yet seem to exist a well-defined concept of "electronic criminal investigation." Nonetheless, it can be defined as an investigation which, regardless to the crime being pursued, either employs information technology or else attempts to obtain elements of electronic evidence by means of computer and information technology.

2. Peculiarities of Electronic Investigations

The fact that electronic investigations are based on information technology or are aimed at obtaining element of electronic evidences has some consequences. The electronic evidences[3] are characterised by intangibility, volatility, easy alterability and, often, ubiquity. This leads to specific features which characterise, or which ought to characterise, the electronic investigations, at least in large part. These features seem to be identifiable as follows:

a) *Identification.* This feature represents the absolute minimum requirement for an electronic investigation. It is defined by the ability to identify the elements of electronic evidence (as in the case of digital photographs) from the equipment that contains them (as in the case of a computer or a digital camera).

b) *Technicality.* The electronic evidence is intangible, i.e. it do not have material substance. For this reason, the acquisition of such a kind of evidence is complex. In particular, there exists the risk that investigative activity itself could alter, unintentionally, the elements of evidence[4]. Moreover, with increasing frequency, within investigations it is necessary to research data that have been hidden by means of steganography. Which is a technique aimed at concealing a message, image, or file within another message, image of file. In other recurring cases, the significant information must be extracted from a message, image, file

[3] See U. SIEBER, *La délinquance informatique*, cit. (note 1), 193-197, as well as E. CASEY, *Digital evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, 2011, 17 et seq.

[4] See G. DI PAOLO, *Prova informatica (Diritto processuale penale),* in *Enciclopedia del diritto,* Annali, vol. VI, Giuffrè, 2013, 738.

whose content, thanks to another technique called cryptography[5], cannot be discovered without the use of a secret key.

For this reason, these investigations require highly expert investigators, capable of seeing beyond mere appearances and of knowing how to conduct an electronic investigation. In addition, the investigators must be equipped with the most appropriate and updated devices and investigation techniques.

c) *Selectivity.* The elements of electronic evidence are often vast in number. For example, a single unit of memory may contain hundreds of thousands of photographs. For this reason, it is necessary to select the material which is really useful for investigation purposes. Such a selection is a very difficult task. Automated computer programs are sometimes used to carry out this selection; thus, it is of fundamental importance that such programs be highly reliable.

d) *Self-Restraint.* Electronic investigations place investigators before a very large amount of data. These data provide a wide spectrum of information, including sensitive data. Moreover, within a single machine (e.g. computer, server, or another information system), there may also be data belonging to third parties outside of the investigation. Since there exists the risk that the investigator could go beyond the limits of a correct investigation activity, leading to an arbitrary and improper acquisition of information, it is necessary that in its activity an investigators exercises self-restraint[6]. In this regard, the creation of an international code of ethics to which the activities of investigators must conform would be a positive step.

e) *Rapidity.* The elements of electronic evidence are volatile. This means that they can be cancelled, written over, or altered in a very brief space of time. This can occur as a result of a human intervention or else as a result of automatic processes already programmed, whether by the person who holds the data or by the software itself. If such elements of evidence can be rapidly cancelled, written over or altered, an effective investigation must be characterised by maximum timeliness. This quality is not always realised, especially in an instance in which the elements of electronic evidence are found in other nations and it is necessary, therefore, to make recourse to traditional forms of international investigative cooperation.

---

[5] See G. ZICCARDI, *Crittografia e diritto,* Giappichelli, 2003.

[6] Brings to light this aspect, R. ORLANDI, *Questioni attuali in tema di processo penale dell'informatica*, in *Riv. dir. proc.*, 2009, 136, as well as P.P. PAULESU, *Notizia di reato e scenari investigativi complessi: contrasto alla criminalità organizzata, operazioni «sotto copertura», captazione di dati digitali*, in *Riv. dir. proc.,* 2010, 802.

f) *Surprise*. As a rule, such investigations can be effective only if they are carried out by surprise[7]. It is not unusual, moreover, that they could never be repeated again.

g) *Transnational in Tendency.* The elements of electronic evidence are characterised by their ubiquitous nature, in the sense that they can be found everywhere. This is true not so much because they can be contained in various machines[8], spread out all over the planet but, above all, because the elements of electronic evidences can be found on the Internet or else in the so-called cloud. This fact leads to extremely relevant problems with regard to jurisdiction, because it often becomes difficult to determine where, in effect, such data are located or found[9].

h) *Proportionality*. Electronic investigations imply a significant violation of fundamental rights, in particular the right to privacy and the right to protection of personal data. Therefore such investigations must agree with the Principle of Proportionality[10], as explicitly required by Article 15 of the Convention of Cybercrime, held by the Council of Europe on 23 November, 2001.

3. Legislation and Electronic Investigations

After a presentation of the main peculiarities of electronic investigations, it is now discussed the Italian legislation which governs them, in particular the Italian

[7] About the defence rights in the context of these investigations, see M. DANIELE, *La prova digitale nel processo penale,* in *Riv. dir. proc.,* 2011, 286 et seq.

[8] To name just a few examples, take into consideration the computer, the tablet, cell phones, printers, scanners, hard disks, the cloud, web sites, compact disks, memory cards, digital cameras, vhs, videos, console video games, smart cards, etc. For an analysis of sources of evidence, see EU/COE Joint Project on Regional Cooperation against Cybercrime, *Electronic evidence guide*, Version 1.0, 18 March 2013, www.coe.int/cybercrime, 16 et seq.

[9] Regarding jurisdictional conflicts see United Nations Office on Drugs and Crime, *Comprehensive Study of Cybercrime, Draft* – Febrauary 2013, 195 et seq., www.unodc.org, as well as M. GERCKE, *Understanding cybercrime: phenomena, challenges and legal response* (ITU publication), September 2012, 235 et seq. Regarding the problematic aspects of jurisdiction within Italian criminal investigations, see F. CAJANI, *Giurisdizione,* in Aterno et al., *Computer forensics e indagini digitali, Experta,* 2011, 157 et seq.

[10] It seems that the principle of proportionality was conceived at the beginning of the last century within German law. Recent developments were also due to The Council of Justice of the European Union. See e.g. Court of Justice, Judgment, 8.4.2014, Digital Rights Ireland e Seitlinger e a., Joined Cases C-293/12 e C-594/12. Among the sources envisaging this principle, notable are Article 52 of the Charter of Fundamental Rights, European Union, and Article 8, European Convention on Human Rights, in the interpretation offered by the European Court of Human Rights.

Code of Criminal Procedure. The fact that these investigations are both inserted into the general picture of criminal investigations, sharing rules with them and subjected to their own rules should be noted.

I. Before all, a general description of the state of criminal investigations in Italy is necessary. In order to provide it, these issues are discussed: a) the sources that discipline the investigations; b) the criminal trial model; c) the function of the investigations; d) the investigative macro-typologies; and e) the subjects who are lawfully assigned to conduct an investigation.

a) *Sources.* The legislation which governs preliminary investigations is principally contained in the Italian Code of Criminal Procedure[11]. The other sources are represented by the Italian Constitution and the Italian law related to the considered matter[12], as well as by European, international, and transnational laws[13].

b) *Criminal trial model.* The Italian criminal trial system is a system of the adversarial type[14]. From this point of view, it provides that:

- The officials that conduct the investigation cannot play the role of judge, because only in this way equidistance between the parties and the judge can be assured;
- Generally, evidence is collected in a public trial, which is the most important phase of criminal proceedings[15];

[11] D.P.R. 22 September, 1988, No. 447 (so-called Codice Vassalli).

[12] Consider, for example, *The Personal Data Protection Code*, Legislative Decree no. 196 of 30 June 2003.

[13] An overview on European sources relevant for Italian Criminal Procedure purposes can be found in R. E. KOSTORIS, *Le fonti,* in R. E. Kostoris (Ed.), *Manuale di procedura penale europea,* Giuffrè, 2014, 5-62.

[14] The Inquisitorial System and the Adversarial System correspond with two abstract models, which are the results of doctrinal analyses. For the most part, in the Inquisitorial System: a) the evidence is gathered by authorities in charge and presented unilaterally; b) the evidence is admissible without any limits; c) the trial is characterised by its secret nature and use of written documentation, in the sense that the judge must decide on the basis of written declarations; d) the accused is presumed guilty; e) preventive detention is always provided for; f) it is held that verification of the facts is best realised only when carried out by a single individual who embodies various functions (judge, prosecutor, defender of the accused). On the other hand, in the Adversarial System, a) the evidence is sought by the prosecutor and the defendant's counsel, not by the judge; b) there are limits to admissible evidence; c) the trial is oral, in the sense that the judge decides on the basis of spoken declarations made in front of him/her during the cross-examination; e) the accused is presumed innocent; f) preventive detention is exceptional rather than the rule.

[15] See G. ILLUMINATI, *Giudizio,* in *Compendio di procedura penale,* in G. Conso, V. Grevi, M. Bargis (eds.), VI ed., Cedam, 2012, 764 et seq.

- An evidence is collected with the adversary method, in a hearing by an independent and impartial judge[16]. the fundamental principle of the separation of phases is in force, according to which the information gathered during the investigation are not admissible in trial. This information can be used by the public prosecutor in deciding whether a suspect should be prosecuted[17], and in relation to the judge's decisions in the dismissal hearing and in preliminary hearing. They are not admissible in trial because the investigations are normally carried out in secret and conducted in a unilateral manner, without using cross-examination. The fact that the information gathered during the investigation are not admissible in trial represents a fundamental rule of the Italian criminal proceedings. However, it should be noted that this rule, and also the central relevance of the trial, do no longer seem to be absolute[18].

c) *Function.* The function of investigations is to verify whether or not to exercise criminal prosecution. The criminal prosecution is the request to the judge to decide about charge, which is to say, to decide whether an accusation on a certain person, with regard to the commission of a crime, is founded or not. From the moment that charges are pressed, the subject under investigation becomes the "accused". Therefore, it is to noted that, during the investigation phase, there is no accused, but only a person under investigation.

d) *Investigative Macro-Typologies.* There are two investigative macro-typologies. On one hand, there are typical investigations. On the other hand, there

[16] The *Italian Constitution* (Art. 111) provides that the process of criminal law is disciplined by the principle of cross-examination in the presentation of evidence. Information on how this principle ought to be upheld not only with reference to declared oral evidence but also in reference to electronic evidence can be found in P. TONINI, *Documento informatico e giusto processo,* in *Dir. pen. proc.,* 2009, 405.

[17] If the accusation of the crime is unfounded, the public prosecutor requests that the judge dismiss it (archiviazione).

[18] It should be noted the fact that, with respect to the time of the activation of the *Italian Code of Criminal Procedure*, the amount of cases where elements of evidence become evidences are significantly increased. Important examples are: a) cases determined by Art. 111, comma 5, Constitution, which is to say, cases of consent of the accused, of ascertained objective impossibility, or by effect of proven illicit conduct; b) cases in which were admitted the so-called "special rites". In particular, in the case of the application of the sentence at the request of the parties, of “abbreviated” (giudizio abbreviato) and of “penal decree of condemnation” (decreto penale di condanna), the judge’s decision is based, with the consent of the accused, on investigation acts used as evidences. With regard to this fact, we must remember that in Italy several criminal trial model exists: an ordinary one, and several special ones. c) Finally, we cannot forget that the elements of evidence constitute the cognitive platform on which the Judge for Preliminary Investigations bases its decision about possible limits on personal liberty.

are atypical investigations. Naturally, both kinds of investigations must respect the principles dictated by national and transnational sources.

Typical investigations are those expressly provided for in the *Italian Code of Criminal Procedure* and consist of four typologies: inspections, searches, seizures, and tapping of conversations or communications.

Atypical investigations (consider, e.g., the shadowing by the police), however, are represented by investigations not disciplined by laws. For these, only a norm exists[19]. It generally permits those investigative activities not governed by laws to be carried out so long as they satisfy the requirements of suitability to insure the verification of the facts. They must not prejudice the moral freedom of the person, and they must realise the adversarial principle between the parties. Furthermore, such atypical investigations must never represent a means by which to elude the typical forms of investigation.

e) *Subjects.* There are three subjects who are lawfully assigned to conduct an investigation: the public prosecutor[20] and the judiciary police[21] on one hand; the defense, on the other.

The public prosecutor and the judiciary police carry out the investigation inside their own specific spheres of activity. The public prosecutor oversees the investigation, but, in certain cases, the judicial police have the power to carry out an investigation on their own.

The contribution of the judge during the investigative phase is only incidental, and in any case, such a judge, which is called the Judge for the Preliminary Investigation (giudice per le indagini preliminari), does not have the power to take initiatives in conducting the investigation itself. His or her job is to act and provide, in those cases allowed by law, on the requests made to him or her by the public prosecutor, by private parties, and by the injured party or victim. In particular, the function of the judge's as guarantor of the fundamental rights of the individual[22] must always be taken into account.

---

[19] Art. 189 *Italian Code of Criminal Procedure*.

[20] The public prosecutor is an integral part of the criminal trial and exercises his function under the oversight of the Ministry of Justice. The public prosecutor must follow the principle of mandatory criminal prosecution (principio di obbligatorietà dell'azione penale).

[21] The judiciary police responds to the Ministry of the Interior (Ministero dell'Interno), but also functionally depends on public prosecutor.

[22] For example, if the public prosecutor plans to conduct wiretapping, he or she must request the judge's authorisation for the preliminary investigation. Only in urgent cases the public prosecutor can act without authorisation from the judge. However, in such an instance, it is necessary that the Judge for the Preliminary Investigation validate the provision issued to the public prosecutor within 48 hours of the action itself.

The defender, too, from the first moment of assignment made in written form of his or her professional responsibility in the case, can carry out investigations. Such investigations are aimed at identifying elements of evidence in favour of the client under investigation, according to the ways and means prescribed by law[23]. They are called defensive investigations (indagini difensive).

II. Once a general picture of the Italian investigative system has been drawn, the legislation specifically provided in the matter of electronic investigations according to the *Italian Code of Criminal Procedure* can be examined. This is a relatively recent discipline.

Despite the fact that electronic investigations have been carried out in Italy for decades, for a very long time no specific rules were considered by the Italian legislator. This lack of specific rules lid to several problems because investigations approaches specifically conceived for electronic investigations were used in the practice, with consequent hermeneutic controversies[24]. Examples of controversial issues are the generation of a clone copy, i.e. the creation of a copy of a database identical to the original, by means of a specific technique, or the e-mail tapping. An aim of the legal doctrine was a clear recognition of the nature of these investigations. In particular, were they activities of the typical kind, or were these investigations as yet undisciplined by laws? Often, the jurisprudence provided conflicting answers.

In 1993, at last, in order to conform the Italian law to Recommendation No. R (89) 9 of the Committee of Ministers to Member States on computer-related crime[25], the Italian legislator made a first modification of the *Italian Code of Criminal Procedure* by introducing a new article (Art. 266 bis). This rule expressly consents the tapping of the flow of communications related to telematics and computer systems. In other words, this article explicitly legitimates an investigation practice whose legitimacy was much discussed in the past.

The next modification of the *Italian Code of Criminal Procedure* in 2008, spurred on by the Convention of Cybercrime of the Council of Europe, was more incisive.

With these new rules, the Italian legislator seems to have made, from a conceptual point of view, a very precise choice. The electronic investigation

[23] Specifically, in libro V, titolo VI bis, Italian Code of Criminal Procedure.

[24] See L. LUPARIA, *I profili processuali (Commento alla l. 18 marzo 2008 n. 48),* in *Dir. pen. proc*., 2008, 717 et seq.

[25] Adopted by the Committee of Ministers on 13 September, 1989. The formulation of Art. 266 bis c.p.p. and its innovative importance did not fail to stir a wide debate in doctrine of criminal law. For an overview of the involved issues, see A. CAMON, *Commento all'art. 266 bis,* in G. Conso, V. Grevi (eds.), *Commentario breve al codice di procedura penale,* Cedam, 2005, 792 et seq.

activities usually carried out (e.g. the generation of a clone copy) are not considered as new kinds of investigation activities. On the contrary, it seems to regard them as mere technical measures in the carrying out of already familiar investigations of the typical kind (inspections, searches, seizures, and electronic wiretapping). In particular, the legislator clarifies that:

The investigations must be performed in such a way as to leave original material intact;

If a copy of data is needed, the investigations must guarantee the identity between the original data and the copied ones;

It is necessary to store the data in such a way that they absolutely cannot be altered;

The legislation, however, did not specify which techniques would, in concrete terms, allow such results to be achieved. This fact seems to imply that the "best practices" of computer forensics[26], being affirmed on an international level, should be used in electronic investigations.

4. Critical issues of electronic criminal investigations

The Italian criminal investigative system actually appears to stand before a kind of epoch transition whose importance has not yet been completely faced by Italian legal doctrine. Besides the fact that electronic investigations lead to a remodeling of known legal institutes and a creation of new ones, they also seem to crack the very foundations of the adversarial model[27].

Moreover, the current Italian legal system which disciplines this area does not seem entirely adequate. A complete examination of all its critical issues is beyond the scope of this paper. Nevertheless, at least the four most significant ones must be discussed here.

A first, capital critical issue is due to the fact that the Italian legislator considers the electronic investigations as simple execution procedures of typical

[26] The so-called computer forensics is a reality in the investigative system, at both the Italian and international level, since several years. Such a discipline deals with the identification, the acquisition, the analysis, and the conservation of electronic evidence. On the origin of computer forensics and its definitions, see G. ZICCARDI, *Le tecniche informatico-giuridiche di investigazione digitale,* in L. Luparia, G. Ziccardi (eds.), *Investigazione penale e tecnologia informatica,* Giuffrè, 2007, 31 et seq.; as well as G. VACIAGO, *Digital evidence,* Giappichelli, 2012, 5-103. Regarding live forensics and postmortem forensics, see D. BUSO, D. PISTOLESI, in F. Ruggieri - L. Picotti (eds.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali,* Giappichelli, 2011, 212 et seq.

[27] An example of important issue is the fact that electronic investigations seem to lead to an eclipse of spoken declarations because digital data seem to leave the oral proof in shadow. In this regard, see R. E. KOSTORIS, in F. Ruggieri, L. Picotti (eds.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica,* cit. (note 26).

investigation (inspections, searches, seizures, and wiretapping). Such an approach does not seem to be convincing. At least some electronic investigations seem to be new kinds of investigations and not mere implementations of typical investigations; again, an example is the generation of a clone copy. Moreover, the rules about typical investigations were conceived with respect to investigations based on use of physical, tangible objects. These rules do not seem to be directly applicable to investigations aimed at acquiring intangible elements of evidence. In addition, they seem to be structurally incompatible with investigations related to cloud computing. The modifications of Italian Code of Criminal Procedure carried out in 2003 and 2008 partially solved the problem, but the question is still open. In the opinion of this author, new typical electronic investigative typologies should be created, in particular in the case of clone copy generation.

Secondly, the Italian legislator does not clarify which legal consequences derive from the failure to employ the best practices of computer forensics. This has raised a wide academic debate, and it has also created a widespread uncertainty in the case law. Does the violation of the best practices originate the exclusion of the evidence obtained? Or does it simply diminish the weight of the evidence[28]? Regarding which, a firm legislative position would have contributed in providing clarity.

A third issue is related to the fact that, until now, the legislator does not consider the atypical electronic investigations. For this reason, new rules aimed at delineating the application field of the Art. 189 of the Italian Code of Criminal Procedure should be adopted. In this way, the recurring doubts about the legitimacy and the consequences of certain atypical electronic investigations could be cast away.

The atypical investigations constitute a rather complex subject. Electronic investigations, in order to be effective, must necessarily keep pace with technological evolution. Therefore, they are subject to continuous new developments. In some cases, technological evolution only leads to new technical systems and/or procedures that can be used to carry out typical investigations. In other cases, the technological development leads to new kinds of atypical investigations. Examples are the use of GPS tracker, or also the so-called on-line searches[29].

In the Italian legal system, atypical electronic investigations imply some very delicate issues. On one hand, they could violate some fundamental rights guaranteed by the Italian Constitution. On the other hand, such investigations

[28] See M. DANIELE, *Caratteristiche della prova digitale*, in F. Ruggieri, L. Picotti (eds*.), Nuove tendenze della giustizia penale di fronte alla criminalità informatica*, cit. (note 26), 212 et seq.

[29] Regarding these subjects the reader could see S. SIGNORATO, *La localizzazione satellitare nel sistema degli atti investigativi,* in *Riv. it. dir. proc*., 2012, 580 et seq., as well as S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche),* in *Cass. pen*., 2010, 2897 et seq.

could violate the rules of the European Convention on Human Rights (ECHR), according to the interpretation provided by the European Court of Human Rights.

If a fundamental right is violated (e.g. personal liberty, inviolability of the domicile, the right to privacy in mail/e-mail correspondence and in other forms of communication), the Italian Constitution states that limitations on such rights are allowed only if there exist both a "*riserva di giurisdizione"* and a "*riserva di legge"*. A „*riserva di giurisdizione"* means that the investigation activity can only be carried out under the condition that a motivated order has been produced by a judge. A "*riserva di legge"* means that the ways and the cases where a right can be violated are defined by a law. Unresolved is the problem which addresses The issues related to the consequences of atypical electronic investigations carried out violating such rights in the absence of the above described Constitution requirements are still debated. According to a school of thought, these elements of evidence cannot be employed in trial. From a different point of view, such elements of evidence could be admissible nonetheless, but it would be necessary to raise the question of constitutional legitimacy related to the Art. 189 of the Italian Code of Criminal Procedure, which generally allows for atypical investigations.

The issues related to the consequences of an atypical electronic investigation carried out violating the rules of the European Convention on Human Rights (ECHR) are perhaps even more complex. The Art. 8 ECHR defends the "Right to respect for private and family life"; such an article has a pivotal role on debate about legitimacy of atypical electronic investigations because they always lead to an invasion of privacy[30]. In regard to this fact, it is necessary to emphasise that, because of current Italian rules in the matter of atypical electronic investigations, Italy seems to be exceedingly exposed to the risk of possible condemnation in the event that judgments were to be handed down by the European Court of Human Rights.

Furthermore, it is imperative to note that, inside the Italian legal system, the ECHR's rules, according to their interpretation provided by the Court of Strasbourg, are an interposed guideline for evaluation of constitutionality within Italian law. Therefore, if an atypical investigation does not conform to ECHR, it would seem to invoke unconstitutionality of the Article that allows for it in a general manner, i.e. the Art. 189 of the *Italian Code of Criminal Procedure*. This because the Art. 117.1 of the Constitution states that the respect of both the constraints dictated by European Union Law and the constraints due to international obligations is compulsory.

Finally, the important issue of conservation of the documentation related to

[30] See 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,* Springer, 2014, 115-128.

electronic investigations is not explicitly faced by the current Italian rules. As a result, the general rules governing the management of documentation provided by other kinds of investigations is also applied to electronic investigations. The standard procedure for some of these investigations allows for documentation in the form of reports, while for others, mere annotations can be sufficient. Furthermore, an audiovisual material can be added to a reports only if it is absolutely indispensable. Such an approach seems to imply that, in Italy, videotaping would not be the first choice or even a habitual means of documentation. The best practices of computer forensics, on the contrary, regard videotaping as a preferred method of documentation in the case of electronic investigations. In some cases the use of videotaping is compulsory. The question seems to be, for that matter, resolvable by way of interpretation. This because, in the case of electronic investigations, the absolute necessity of videotaping would be determined by the electronic character of the investigation itself. An intervention by legislator, although not yet necessary, would seem opportune for a definitive clarification on this point.

5. Conclusion

The criminal electronic investigations are more and more often used in Italy. Nevertheless, the regulation provided by the Italian Code of Criminal Procedure seems to be not completely adequate. In particular, the Italian legislator considers the electronic investigations as mere technical measures in the carrying out of already familiar investigations of the typical kind (inspections, searches, seizures, and electronic wiretapping). This fact can be criticised because, at least in some cases (e.g. the generation of a clone copy), it seems that electronic investigations seem to be new kinds of atypical investigation activities instead. Moreover, atypical electronic investigations imply some very delicate issues about their compatibility with the fundamental rights.

For these reasons, it would be desirable an intervention by legislator aiming at better regulate both the typical and atypical electronic investigations.