Collezione di Giustizia Penale

dedicata a Massimo Nobili
e diretta da Marcello L. Busetto, Alberto Camon, Claudia Cesari,
Enrico Marzaduri, Daniele Negri

7

Each volume published in this series has been approved by the directors and – with the exception of conference proceedings – submitted for double blind peer review in accordance to the series' regulation. The regulation and the records pertaining to the review of each book are kept by the publisher and by the directors.

DIGITAL FORENSIC EVIDENCE

TOWARDS COMMON EUROPEAN STANDARDS IN ANTIFRAUD ADMINISTRATIVE AND CRIMINAL INVESTIGATIONS

edited by
Michele Caianiello and Alberto Camon

Wolters Kluwer CEDAM

Printed by GECA s.r.l. - Via Monferrato, 54 - 20098 San Giuliano Milanese (MI)

This publication was funded by the European Union's HERCULE III programme.

Table of contents

LAURA BARTOLI-GIULIA LASAGNI

THE HANDLING OF DIGITAL EVIDENCE IN ITALY

Katalin Ligeti-Gavin Robinson

THE HANDLING OF DIGITAL EVIDENCE IN LUXEMBOURG

LORENA BACHMAIER WINTER

THE HANDLING OF DIGITAL EVIDENCE IN SPAIN

Laura Bartoli-Giulia Lasagni

ANTIFRAUD INVESTIGATION AND DIGITAL FORENSICS: A COMPARATIVE PERSPECTIVE

Michele Caianiello

CONCLUSIVE REMARKS
ANTIFRAUD INVESTIGATIONS AND RESPECT FOR FUNDAMENTAL RIGHTS FACED WITH THE CHALLENGE OF E-EVIDENCE AND DIGITAL DEVICES

Laura Bartoli-Giulia Lasagni *

THE HANDLING OF DIGITAL EVIDENCE IN ITALY

Overview: 1. The digital investigation: a regulatory overview. – 1.1. Constitutional framework. – 1.2. Regulatory framework: police investigation. – 1.3. Regulatory framework: the expert consultant. – 1.4. Technical standards. – 1.5. Conundrums. – 1.6. Privileged information. – 1.7. – Chain of custody. – 2. Investigating Authorities. – 2.1. Law Enforcement. – 2.2. Digital Forensics Consultants. – 3. Defence Rights: Information and Right to be Heard. – 3.1. Defensive Investigations. – 3.2. Consent of the Accused. – 3.3. Remedies. – 3.4. Third-Party Rights. – 4. Digital evidence at trial. – 4.1. Admissibility. – 4.2. Production of evidence in different proceedings.

1. *The digital investigation: a regulatory overview*

1.1. *Constitutional framework*

The Italian Constitution was approved in 1947 and entered into force in 1948. Unsurprisingly, the text was not concerned at all with the notion of digital information, and the relevant portions of the text have not been amended since. The principles that apply to the digital investigation are therefore the same that can be applied to any sort of investigation, and in particular: art. 14, declaring the inviolability of domicile; art. 15, protecting freedom and confidentiality of correspondence; art. 24, acknowledging defense as an inviolable right, art. 111, granting the right to a fair, adversarial trial.

This approach, nowadays, can come across as outdated. The domicile enjoys constitutional protection, as does the right to free and covert communication; the private sphere of an individual,

* This work is the result of a joint research carried out by both authors in the Devices Project. For the purpose of the present Chapter, L. Bartoli is the author of §§ 1 and 4, and G. Lasagni is the author of §§ 2 and 3.

however, is not directly covered as such. Moreover, the Italian constitutional Court has been rather conservative in its interpretation, especially if one compares its jurisprudence with the one of the German constitutional Court: the latter has been forging new fundamental rights to limit the legislature, whereas the former has been more passive.

Against this background, legal scholars have tried to adapt the old notions to meet new challenges, and the inviolability of domicile seemed the best provision to expand. With a little imagination, any device could be construed as a digital domicile, that – according to these theories – should be granted the same constitutional guarantees of the traditional domicile. However, this attempt has not been overwhelmingly convincing: the notion of "domicile" is not fully satisfactory, for data travel half around the world more often than not, and end up stored in foreign servers [1].

The Constitution alone does not answer all the issues that the digital revolution has brought forward, hence the courts are increasingly resorting to European sources to grant constitutional footing to more flexible principles such as proportionality and privacy. The main point of reference has become art. 8 of the European Convention on Human Rights; unlike the Dutch or the Luxembourgian system, the Italian body of laws does not allow for a direct application of international sources. The parties cannot invoke art. 8 ECHR to set aside a specific national provision; however, the courts should interpret national law in the closest possible accordance with the principles of the Convention, or can ask the Italian Constitutional Court to annul an internal provision because it infringes upon the rights granted by the Convention [2].

---

[1] For more references on the Italian debate on the extended notion of "domicile" and its effectiveness, see G. LASAGNI, *Banking Supervision and Criminal Investigation. Comparing the EU and the US Experience*, Springer, Cham, 2019, p. 329 ff.; or, in Italian, S. SIGNORATO, *Le indagini penali informatiche. Lessico, tutela dei diritti fondamentali, questioni generali*, Giappichelli, Torino, 2017, p. 51 ff.

The European Union is trying to tackle the problem with the proposed introduction of the European Production and European Preservation orders. For an overview on the set of issues that this peculiarity entails see L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Eurojus*, 2019, p. 96 ff.; M. DANIELE, *L'acquisizione delle prove digitali dai* service provider*: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. de Dereito Processual Pen.*, vol. 5 (2019), f. 3, p. 1277 ff.

[2] See M. LUCIANI, (entry) *L'interpretazione conforme a costituzione*, in *Enc. dir.*, *Annali IX*, Giuffrè, Milano, 2016, p. 451 ff.

A different mechanism could apply for EU sources, within the scope of EU attributions. In that case, national legislation can be put aside if it is in contrast with a directly applicable European provision, which is to say: sufficiently detailed and that does not need further implementation. These requirements, however, seem hard to satisfy when it comes to fundamental rights; in that area, the national judge can apply for a preliminary judgment to the European Court of Justice, or to the Italian Constitutional Court. The provisions of the Charter of Fundamental Rights of the European Union may not be directly applicable, but they come up more and more often as they are used by courts to interpret and apply national law. In the domain of digital investigations, art. 52 § 1 of the CFREU has sometimes served as a stronger basis for the proportionality principle [3].

European sources are key in giving some degree of constitutional footing to privacy and proportionality, but their transformative power is limited: they help the practitioners in arguing more considerate solutions, but they have not yet induced the Italian legislator to consistently pursue them, or the Constitutional Court to consistently enforce them.

1.2. *Regulatory framework: police investigation*

Criminal and administrative proceedings do not regulate digital investigations as such. The Italian legislator made minor amendments to both branches as soon as some of the issues surfaced, but never even try come up with new, specific measures. The rules on inspections, searches and seizures, after being applied were just extended [4].

At the administrative level, there is no specific mention of digital investigations during on-spot checks. A statute issued in 1994 provides for the validity of all digital records as long as they can be printed out; during a control, the police should therefore gather a hard copy [5]. This

[3] Cass., Sez. VI, 13 March 2019, n. 37639, in *DeJure*; Cass., Sez. VI, 14 February 2019, n. 41974, in *SentenzeWeb*; Cass., Sez. III, 29 September 2009, n. 42178, in *C.e.d.*, n. 245172-01.

[4] For some critical observation on this strategy, see *infra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics: a comparative perspective.*

[5] D.l. 10 June 1994, n. 357, art. 7 § 4-*ter*, transposed into law by l. 8 August 1994, n. 489.

provision is still in force, and the relevant soft law mirrors it: all the registries that the taxpayer is supposed to keep shall be printed and provided to the *Guardia di finanza* on paper [6]. The rules on administrative proceedings for damage to the treasury also allow for the seizure of documents «in digital format».

When the occurrence can be construed as a crime, the code of criminal procedure shall apply [7]. When it entered into force in 1988, it did not envisage digital evidence as such; the first reference to digitally stored information was added 20 years later, in 2008, with the law that implemented the Budapest convention on cybercrime [8].

On the one side, it was a leap forward. Rules on inspection, searches and seizures now contain a specific reference to digital material, and the same rules of the "physical world" apply to data according to clear legal provisions and not to the practitioners' best guess. The public prosecutor can inspect a personal computer or a network when «it is necessary to find traces and other material items of the offence» (art. 244 § 1); she can order a search «if there are reasonable grounds to believe that data, information, software or any other traces relating to the offence are stored in a computer or electronic system» (art. 247 § 2). Both measures have been adapted but, if the difference between the two of them is clear with regards to non-digital situations, it is much harder to grasp the respective area of application when it comes to computers. Inspecting the premises, for instance, means that the prosecutor needs to ascertain the *status quo*, whereas searching implies a "hands-on" activity: the prosecutor – or, more often, the police upon the prosecutor's mandate – will literally search for the «the *corpus delicti* or other material items related to the offence» (art. 247 § 1). When it comes to data, however, it is hard to imagine a purely "hands-off" analysis of the contents of a system; the room for the inspection basically disappears, or it is limited to an exterior observation of the device [9].

---

[6] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 23.

[7] For more on this point, see § 5.

[8] L. 18 march 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».

[9] See A. CAMON, *I mezzi di ricerca della prova*, in A. CAMON-C. CESARI-M. DANIELE-M.L. DI BITONTO-A. NEGRI-P.P. PAULESU, *Fondamenti di procedura penale*, CEDAM, Padova, 2019, p. 357; S. SIGNORATO, *Le indagini digitali*, Giappichelli, Torino, 2018, p. 206 f.

Continuing along the lines of the law, if the search has brought to light some relevant material, the prosecutor may order the seizure of «the *corpus delicti* or other material items related to the offence» (art. 253 § 1). If the relevant material is «held by providers of computer, electronic and telecommunication services», the public prosecutor may order the seizure by copy, to maintain «the standard provision of such services» (art. 254-*bis*). All of these measures may be ordered through a reasoned decree issued by the «judicial authority», a comprehensive way to indicate the prosecutor during the investigation, or the judge during trial.

In case of urgency, however, the police can act *motu proprio* in two cases. The first hypothesis is the need to search for evidence when the accused is caught red-handed (*in flagrante delicto*); if the police officers have reasonable cause to believe that «data, information, software or traces anyhow related to the offence» could be tampered with or deleted, they can search the «informatic system» without the prosecutor's decree (art. 352 § 1-*bis*). The second case deals with another kind of urgency; in this scenario, police officers are the first responders at the scene and the prosecutor has not yet been able to intervene and take full charge of the investigation. The judicial police is therefore tasked with preserving all relevant elements that could be «lost or anyhow modified» by waiting the proper appointment of the prosecutor, or her intervention in the investigation (art. 354 § 2). The police officers, in this case, have to protect the original data and prevent their alteration; if it is possible, they can do so by copying data they fear would disappear; they can also seize «the *corpus delicti* and the objects related to it». If a seizure occurs, the police officers have to notify the prosecutor within 48 hours, that has 48 hours upon receipt to confirm the measure or revoke it.

Thanks to the ratification of the Budapest convention, digital investigations have an explicit legal base and all of the provisions mentioned so far contain one additional warning: in inspecting, searching, seizing, the practitioners shall adopt «technical measures capable of guaranteeing the preservation of the original data and preventing their alteration» (art. 244 § 2, art. 247 § 1-*bis*, art. 352 § 1-*bis*). When the copying process is mentioned (art. 254-*bis* and art. 354 § 2), the provisions contain another *caveat*: the duplicate shall be obtained «following a procedure that ensures that the copies are identical to the original and that they cannot be modified».

Both these precautions directly stem from the Budapest convention, whose art. 19 stresses the need to «maintain the integrity

of the relevant stored computer data» in searches and seizures; the objective is as important as difficult to ensure: even a trifle – *e.g.*: turning the device off – could alter the original set of information, potentially undermining the analysis.

Ensuring integrity can mean different things in different scenarios: searching a file on a thumb drive may not be the same as searching for volatile data that reside in the RAM. The first is permanent, the second ones disappear as soon as the device is powered off. The set of circumstances that the agents must operate under influences the method, along with the type of information that they have to look for. Therefore, the legal provisions do not delve into technical details: fixing just one method would be very risky, if not outright mistaken; regulating all possible methods would be probably a useless effort. Keeping up with the racing technology is a difficult task, especially for a legislative body: fixing an objective and leaving some degree of leeway when it comes to the methods can be a good compromise, one that also allows to choose the most effective approach with respect to the single case.

In this domain, soft law is probably the most effective tool, but no standard has been strong enough to serve as a national guideline, recognized by all practitioners and by the courts. As far as antifraud investigations are concerned, the matter is simplified because the police force investigating is, more often than not, the *Guardia di finanza*, which has its own guidelines in place [10]. However, the courts do not take them into account while assessing the reliability of evidence, nor they seem to be aware of their existence. In practice, it is very hard to discredit the methods that the police has selected: the courts would simply answer that the law does not favor any particular procedure, therefore practitioners can act however they deem better.

In short, the legislator has importantly set an objective, but has substantially failed at giving it a tangible, measurable content, and because of this lack of practical fallout, the reform went almost unnoticed for little less than a decade. For instance, it took roughly 10 years for the courts to acknowledge that data could be autonomously seized, and that they do not necessarily follow the device's path. Until 2017, the physical device could have been seized, copied, given back to the rightful owner; of course, all

[10] They are part of the Circular n. 1-2018, whose parts on computer forensic operations will be closely analyzed.

information would be at the disposal of the investigator nonetheless, and the device was only given back because it did not have any autonomous evidentiary value. However, the courts consistently denied the right to a judicial review [11], that is normally bestowed upon the «accused, the person from whom objects have been seized and the person who would be entitled to their restitution» (art. 257). The physical object had already been given back and therefore, according to this perspective, there was nothing left to claim, as if data did not matter at all. In 2017, the Supreme Court reached a long awaited, different conclusion, and it did so by examining the provisions that were amended in 2008: the decision proclaimed the independent value of digitally stored information and opened to the judicial review, but only if the concerned individual shows a concrete and actual interest to the restitution of the data [12]. The decisions that came after have seldom recognized the right to privacy as a strong enough interest to trigger the judicial review [13].

1.3. *Regulatory framework: the expert consultant*

When the judge or the parties want to bring in a digital forensic consultant, different rules apply.

On the administrative branch, the need for an expert consultant should be hampered by the specific guidelines of the *Guardia di finanza*. Circular n. 1-2018 recommends an accurate selection of the personnel to involve in the check: when it is reasonable to expect the gathering of digital evidence, the commanding officer should pick at least one agent with the appropriate degree of expertise (see

---

[11] Cass., Sez. Un., 24 April 2008, n. 18253, in *C.e.d.*, n. 239397-01; on the subject, see the observations of S. Carnevale, *Copia e restituzione di documenti informatici sequestrati: il problema dell'interesse ad impugnare*, in *Dir. pen. proc.*, 2009, p. 469 ff.

[12] Cass., Sez. Un., 7 September 2017, n. 40963, in *C.e.d.*, n. 270497-01; on the decision, see the observations of L. Bartoli, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. (web)*, 2018; A. Mari, *Impugnazioni cautelari reali e interesse a ricorrere nel caso di restituzione di materiale informatico previa estrazione di copia dei dati*, in *Cass. pen.*, 2017, p. 4303 ff.; G. Todaro, *Restituzione di bene sequestrato, estrazione di copia, interesse a impugnare: revirement delle Sezioni Unite*, in *Dir. pen. cont. (web)*, 2017.

[13] For a notable exception, see Cass., 21 November 2017, n. 1822, in *SentenzeWeb*. The investigators had seized the target's entire email correspondence and her phone; the Court of Cassation declared that the personal and reserved nature of the material fully justified a judicial review.

Section 2). To rationalize the effort, the guidelines differentiate between "simple cases" and "hard cases". For the simple cases, the head of the office can decide to deploy agents with basic informatic skills; for more complex investigations, the head of the office should select personnel trained of computer forensics and data analysis.

The rules on administrative proceedings for damage to the treasury, however, allow for the appointment of an expert consultant «when the public prosecutor shall proceed to ascertainments that require specific skills» [14]. As for the selection of the expert, the provision makes reference to the rules of the code of criminal procedure.

During a criminal investigation, the parties are free to hire a technical consultant whenever they need one. The prosecutor could have the police carry out the operation "in-house", but if she requires a higher degree of expertise, she can appoint an expert consultant. If the ascertainment is deemed repeatable (art. 359 c.p.p.), it can be executed by the sole prosecutor's expert, without consulting the defense. If the ascertainment is deemed non-repeatable (art. 360 c.p.p.), the material will be directly put in the trial dossier (art. 431 c.p.p.) and will be used for the final decision; therefore, it is necessary to involve the defense at an early stage. The prosecutor shall give notice to the defense, that can participate to the operations with her own consultant or ask that the ascertainment takes place in front of a judge, in a special evidentiary hearing (*incidente probatorio*).

The defense lawyer has the same powers as the prosecutor when it comes to hiring experts, that can perform repeatable and non-repeatable ascertainments (in this case, the prosecutor shall be informed and can exercise the faculties of art. 360 c.p.p.). However, she cannot autonomously seize computers or conduct searches. She can inspect public places; the concerned individual or the court can grant access to the premises (art. 391-*sexsies* and 391-*septies* c.p.p.).

Finally, if the trial judge requires a technical consultant, she can appoint an impartial expert: she will carry out the assigned task and give expert evidence in open court, in front of both parties (art. 220 ff. c.p.p.). Any party to the trial can appoint their own consultants: they have the right to join the court-appointed expert during the operations and give suggestions and observations that shall be

[14] Art. 63 codice della giustizia contabile.

mentioned in the record. Normally, this expertise comes in question when it is necessary to have the data analyzed and interpreted; in most cases, the material should have already been gathered by the prosecution or by the defense during the preliminary investigation.

1.4. *Technical standards*

As mentioned above, there is no widespread, national standard on digital investigations as such. Of course, the problem is not a technological one; standardizing agency and police corps all around the world have come up with best practices adapted to a vast range of situations and subjects: first responders operating on a device, live forensics, cloud forensics, smartphone forensics and so on. The issue is rather a political one: the choice has so far been that of not explicitly regulating these aspects.

However, the antifraud domain constitutes an exception in this regard, not because of a different legislative intent, but because of a regulatory effort of the *Guardia di finanza*, that operates horizontally in the field. This police force is concerned with custom controls, fiscal inspections, investigations on damages to the treasury and criminal antifraud investigation, effectively occupying all the spectrum of administrative and criminal proceedings. In 2018, the *Guardia di finanza* published an updated edition of its operational handbook [15], which contains a number of detailed provisions about how digital material should be gathered.

First of all, the guidelines underline the importance of preparing every action: before leaving for a check, the commanding officer should go through a checklist aimed at summarizing what the police already knows of that individual, including the allegations of wrongdoing. Once the agents get on the scene, they should identify all possible repositories of information at a given location. For instance, searching the computer could not be enough, because all the "black book" could be kept on a separate hard drive. The first task, then, should be the census of all potential sources.

Once all devices are accounted for, the agents should gather the

[15] Comando generale della Guardia di Finanza, III Reparto Operazioni – Ufficio Tutela Entrate, *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali* (Circolare n. 1/2018), Vol. II, online at *gdf.gov.it* (hereinafter: Circular n. 1-2018).

relevant material. Here, the suggested procedure differs greatly according to the complexity of the case. When the ascertainment does not appear particularly intricate, the captain can deploy personnel with basic IT skills, and they will have to go through the files together with the subject of the search, or with someone from the IT department of the firm [16]. All operation must be described in detail, and every passage has to be accounted for. The underlaying rationale is clearly stated: every interaction with the digital material must be auditable by the defendant, by third parties and ultimately by the judge; everyone should be able to ascertain or to question the reliability of the technical methods and of the results of the investigation.

When the relevant files are identified, they should be copied twice; one of the copies shall remain untouched and preserved for the records, to allow any subsequent new analysis in case issues about authenticity should surface. The most interesting information can be directly printed out. All seized items have to be mentioned in the police report, which the subject and the agents will sign, together with the hardware containing the copies.

For hard cases, the rules are stricter. First of all, the police agent should be an expert in computer forensic and data analysis. She can decide what to do: either copy the entire memory and create a bit-stream image (which is the best practice from a forensic point of view); either select only the relevant files; in any case, the authenticity should be ensured by calculating and comparing the hash value for every file. The selection of material should then be archived and transferred on a different mass storage unit.

Afterwards, the investigator should analyze the data. As we saw, it is not outlandish to print out all relevant material and acquire the hard copy. If so, the following phase of interpretation and analysis will not involve digital techniques.

Let us assume, though, that the data has been duplicated and maintained on digital format. The data now has to go through a second stage to be analyzed and interpreted. In the administrative proceeding, this phase seems to go undetected. The guidelines only mention a detail: the analysis should be carried out on a working copy of the information, so that one of the authentic copies is preserved for the record. It will serve as a matrix: whoever needs to

[16] The easy-case scenario is regulated by Guardia di Finanza, Circular n. 1-2018, vol. II p. 29.

analyze the information and verify the conclusions will be able to extract a new working copy.

In the criminal proceeding, the approach varies according to the subject who has to perform the analysis. If the prosecution decides to deal with the matter "in-house", the best standard available is the aforementioned circular. However, the parties or the trial judge could decide to appoint a consultant for this task. During the investigation, the rules can change according to the status of the operation: it could be labeled as repeatable, or as unrepeatable. The line between the two categories is thin, but – as mentioned above – the safeguards differ greatly. Repeatable operations can be independently carried out by a party, without involving the other one nor the judge. The results will be kept in the prosecutor's dossier, and they will be presented in court after an admissibility ruling and after the expert witness testifies on her findings. Non-repeatable operations, on the contrary, have to be notified to the opposing party, that has the right to participate with her own consultant, or to ask for a special evidentiary hearing. In any case, the results of this operations will end up in the trial dossier: the judge will know them since the beginning. If the rules are violated, however, the judge will have to disregard the evidence.

The distinction bears serious consequences, but it is pretty much left in the hands of the public prosecutor, especially in the domain of digital forensic analysis: the jurisprudence has often upheld that the analysis of a device is not non-repeatable operation – regardless of how it is conducted [17]. The conclusion, though, seems disputable. Data analysis is indeed repeatable if the original (or a "virgin" copy) is still available: in this case, the counterpart will be able to check every step of the way that led from the raw material to the conclusion. If the material has been compromised, it is impossible to repeat the operation.

1.5. *Conundrums*

Necessity and proportionality are general requirements of all seizures, including those targeting data. The jurisprudence derives these constraints from the regulation of precautionary measures,

[17] Cass., sez. V, 16 November 2015, in *C.e.d.*, n. 266477-01; Cass., sez. II, 1 July 2015, n. 29061, in *C.e.d.*, n. 26457-01.

where they are explicitly set by law [18]; fewer decisions assume art. 52 § 1 of the CFREU as a legal basis for the proportionality clause, unequivocally putting it on constitutional footage [19]. Applying these principles to seizures means that the investigators (and ultimately, the prosecutor) cannot apprehend more than it is strictly necessary to ascertain the fact. The connection does not always have to be the closest, but it must be present and specifically explained by the authority [20]. Moreover, time is a relevant factor in establishing proportionality: for instance, it may be necessary and proportionate to seize the device, but not for longer than it takes to copy it. Besides, the investigators should choose the least intrusive – and yet adequate – means to the end.

And yet, technically speaking, the best way to ensure the repeatability of the analysis, to make sure that all relevant information have indeed been gathered, and to be able to put the findings in full context is to create a mirror-image of the device's memory. For all of these reasons, all technical standards would recommend the acquisition of the full set of data, whereas the legal golden rule is to interfere with the individual's privacy as little as possible, and only insofar as necessary.

This friction is fruit of a hypocritical legislative choice: in the physical world, the search is instrumental to ensure that the seizure is limited to the strictly necessary; the reasoned decree authorizing the measure should clearly explain the proportionality and necessity of the investigative action. In the digital world, this solution makes little sense. The decree can very well contain all reasons for the investigators to seize a relevant portion of data, but the safest option is to collect the entire memory anyway: going through the digital material on-spot, though, could be too time consuming, it could alter

---

[18] Cass., sez. un., 29 January 2015, n. 31022, in *C.e.d.*, n. 264089-01. See also: Cass., sez. V, 9 September 2019, n. 42765, in *C.e.d.*, n. 276908; Cass., sez. VI, 13 March 2019, n. 37639, in *DeJure*; Cass., sez. VI, 14 November 2018, n. 4857, in *SentenzeWeb*; Cass., sez. VI, 19 January 2018, n. 9989, in *C.e.d.*, n. 272538-01; Cass., sez. V, 21 November 2017, n. 1822, in *SentenzeWeb*; Cass., sez. VI, 24 February 2015, n. 24617, in *C.e.d.*, n. 264093-01.

[19] Cass., sez. VI, 13 March 2019, n. 37639, in *DeJure*; Cass., sez. VI, 14 February 2019, n. 41974, in *SentenzeWeb*; Cass., sez. III, 29 September 2009, n. 42178, in *C.e.d.*, n. 245172-01.

[20] Cass., sez. VI, 13 March 2019, n. 37639, in *DeJure*; Cass., sez. VI, 5 December 2018, n. 1364, in *SentenzeWeb*; Cass., sez. VI, 14 November 2018, n. 4857, in *SentenzeWeb*; Cass., sez. VI, 11 November 2016, n. 53168, in *C.e.d.*, n. 268489.

the original data and it could be ineffective; only the easy cases allow for the traditional sequence "search first, then seize". In all other cases, the progression is normally reversed: instead of searching in order to target the seizure, investigators seize in order to search.

In one case, the *Guardia di finanza* (so, the police force operating under the Circular 1-2018) seized all the corporate computers and thumb drives of six suspects accused of false accounting for the year 2016. All defendants pointed out that the seizure of all corporate devices was not proportional to the charge, definitely more limited in scope. The prosecution simply alleged that the case was too complex to perform a targeted seizure, and the Court sided with the investigators [21], also given the enormous amount of technical discretion that is granted to the agents. The Court of cassation made no mention of the Circular 1-2018, nor it imposed a time limit on the retention of the entire collection. All proportionality concerns were simply erased by the alleged complexity of the case.

Other decisions, however, are more sensitive. A couple of recent judgments have explicitly stated that mirror imaging the device's memory does not violate the proportionality principle: it is true that the quantity of gathered material certainly exceeds the needs of the investigation, but it is also true that the measure needs to be evaluated within its dynamic, as a preliminary stage to the subsequent identification of the relevant material [22]. In other words: proportionality, in its quantitative meaning, has to be protected after the gathering, making sure that there is an adequate selection in place. Meanwhile, what must be protected is proportionality in its temporal sense: the full set of data must be preserved for as long as it takes to carry out the analysis, and no longer [23].

The setting would be good enough if the law had regulated an *ex post* selection mechanism, but the traditional regulation of seizure does not contemplate anything like it. The role, now, is occasionally picked up by the tribunal charged with the re-examination of the seizure: the review can be triggered by the defense, if it proves to have a concrete and actual interest to the exclusive possession of the data. This

[21] Cass., sez. V, 17 May 2019, n. 38546, in *C.e.d.*, n. 277343-01.

[22] Cass., sez VI, 4 March 2020, n. 13166, in *SentenzeWeb*; Cass., sez VI, 4 March 2020, n. 13165, *ivi*.

[23] Both decisions make reference to Cass., sez. VI, 14 November 2018, n. 4857, in *SentenzeWeb*, that emphasizes the need for a time limit to the retention of all data in order for the seizure to be proportional.

solution, however, is not fully acceptable: first of all, the right to a judicial review on the legitimacy of the measure is somehow restricted – often the right to privacy is not recognized as a sufficiently intense interest [24]. Moreover, this process can only be triggered with ten days upon the enforcement of the seizure (art. 324): more often than not, it is completely normal that the analysis has not yet been carried out to completion, and that the retention of the full set of data would still be regarded as necessary. Finally, the re-examination has been conceived as a remedy for an illegitimate seizure: it is not regulated to adequately run a selection procedure – for instance, it cannot order the destruction of copied material [25].

Another tool that has occasionally served as selection procedure is the special evidentiary hearing. In a case, the prosecutor decided to use the procedure provided by art. 360 (non-repeatable ascertainment) to gather data. The defense subsequently applied for a special evidentiary hearing – as it is its right, as provided by art. 360 § 4 – and the entire procedure was supervised by the preliminary investigation judge, which also presided over the selection procedure. This solution is perfectly adequate: it allows the involved party to get the material they want and exclude the rest from the public record. However, as mentioned above, the prosecutor is in no way obliged to qualify the collection of data as a «non-repeatable ascertainment»; she can, if she wants to, but the direct execution of the measure by the police or by an expert consultant – without previously warning the defense – is equally acceptable, and sometimes even necessary. For instance, the accused could try to destroy or alter the material: as the biggest bankruptcy in European history was unfolding, the management at Parmalat was literally smashing computers with a hammer to prevent the collection of evidence [26].

Such a crucial step cannot be left to the occasional generosity of the prosecutor: it deserves to be established by law. Scholars – and,

---

[24] For a recent example, see Cass., sez. II, 17 January 2020, n. 6998, in *SentenzeWeb*. In an investigation for false testimony, the police seized all data of the computer systems of five companies: the defense argued that such a broad seizure impacted on the right to privacy and to the companies' intellectual property rights. The Supreme court rejected the appeal as lacking a precise enough interest.

[25] Cass., sez VI, 4 March 2020, n. 13166, in *SentenzeWeb*; Cass., sez VI, 4 March 2020, n. 13165, *ivi*.

[26] P.F. FEDRIZZI, *La confessione del contabile: martellate sul computer*, in *repubblica.it*, 29 December 2003.

sometimes, even the Supreme court – have been advocating for different amendment projects: either allowing a special evidentiary hearing for all digital seizures [27], or regulating a selection procedure modeled on the discipline of interception of communications [28].

1.6. *Privileged information*

The clash between technical standards and legal protections is particularly palpable when the data to collect are privileged.

The situation that has been more frequently examined by courts is the search and seizure of a journalist's devices. Under Italian law, professional journalists enjoy can refuse to disclose the identity of their sources (art. 200 c.p.p.). The privilege can be pierced, and the journalist may be ordered to reveal the source when the information is indispensable to prove the crime and its reliability can be tested only by identifying the source. The law also regulates seizures when the concerned individual can claim professional privilege: the authority performing the measure has to request the handover of the relevant data, and the subject must abide unless she declares in writing that the relevant information is privileged.

The case law has clarified that the agents do not have to warn the subject about the possibility to claim privilege: it is up to the single journalist or professional to invoke the confidential nature of the material, and she has to do that in written form. If there are doubts on the existence of privilege, the «judicial authority shall proceed with the necessary ascertainment [...]. If the declaration is groundless, the judicial authority shall order [the] seizure».

If the professional does not invoke privilege and refuses to hand over the data, the normal provisions about searches and seizures apply. Due to the jurisprudence on art. 10 ECHR, however, part of the case law explicitly prohibits the «indiscriminate apprehension of the entire data archive», *id est*: the mirror imaging of the device. According to this set of decisions, proportionality should be taken very seriously also in its quantitative meaning; therefore, the agents performing the measure should always search the archive on the spot

---

[27] F. Iovene, *Perquisizione e sequestro di computer: un'analisi comparatistica*, in *Riv. dir. proc.*, 2012, 1616, which advocated for an amendment to open a special evidentiary hearing to select digital material.

[28] L. Bartoli, *Sequestro di dati a fini probatori*, cit., p. 17 f.; in the same direction: Cass., sez. V, 27 ottobre 2016, n. 25527, in *DeJure*.

and be rigorous in seizing only what is necessary [29]. Other, more recent judgements, however, have partially reversed the trend, affirming the need to evaluate mirror imaging as a part of a «dynamic» process aimed at an *ex post* selection [30], also when it comes to journalists.

During administrative checks, all the fiscal documentation cannot be cloaked in professional privilege. If the accountant could refuse to show all financial records to the police, every antifraud investigation would be doomed; on the contrary, the administration is entitled to see a certain amount of fiscal and financial records. Therefore, case law has been careful in limiting the scope of privilege: it covers all information that do not relate to the fiscal or economic interests of the professional and her client. A blind protection of the privilege – according to the Court of Cassation – would infringe upon art. 53 of the Italian Constitution, which provides that «every person shall contribute to public expenditure in accordance with their capability».

From the operational standpoint, the officers should interrupt their activities when the professional claims that the documents being checked are privileged. The police can immediately investigate the nature and scope of the privilege, interviewing the professional and/or whoever can provide useful information on the privileged nature of the documents. The agents cannot decide by themselves that privilege does not apply: they need an authorization of the Public Prosecutor, stating that the privilege does not apply and ordering the immediate exhibition of the supposedly privileged material [31]. In case of urgency, the agents shall preserve, but not open or look at the content of the allegedly privileged information. The same goes for digitally stored data, as explicitly stated by the Circular n. 1, 2018 [32].

1.7. *Chain of custody*

The Italian legal system does not contemplate the notion of a U.S.-style chain of custody; instead, it provides for a general regulation about

[29] Cass., sez. VI, 19 January 2018, n. 9989, in *C.e.d.*, n. 272538; Cass., sez. VI, 24 February 2015, n. 24617, *ivi*, n. 264092.

[30] Cass., sez VI, 4 March 2020, n. 13166, cit.; Cass., sez VI, 4 March 2020, n. 13165, cit.

[31] The need of such an authorization is spelt out by d.P.R. 26 october 1972 n. 633, art. 52 § 3.

[32] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 26.

reporting, that is technology neutral. The code of criminal procedure establishes a duty to report on searches, seizures and non-repeatable ascertainment (art. 373 and art. 357 c.p.p.). The report shall be signed and stored in the dossier, with all other pieces of documentation concerning the case. The degree of detail is pretty much left to the single practitioner: in theory, reports on seizures should precisely list what was taken, by whom, how was it stored and sealed, who is in charge of it (art. 81 disp. att. c.p.p.). In practice, however, the onus could be satisfied by reporting the seizure of a personal computer, with no reference at all to what it contains.

After the gathering, the material shall be sealed (art. 260). Objects can be stored in bags and envelopes, that have to be closed, secured with the seal of the office and signed by the judicial authority and its assistant. Data can be either stored in the original device, either copied to ensure their preservation. The law repeats the usual warning: the copying techniques shall ensure the authenticity of the duplicate and guarantee that data cannot be re-written or modified. The device, the data or both have to be sealed, in order to ensure their authenticity.

All seized material (digital or non-digital) is normally stored at the prosecutor's clerk's office or at the Court's registry. When data are copied, sealed and safely stored, however, the originals can be kept outside of those offices (notably: given back to the proprietor).

When the seized items are touched again, the seals must be checked by the authority and removed. After the operations, the items shall be sealed again and re-signed by the proceeding authority and its assistant.

This system is notably tailored for objects, but is not the best solution available for seized digital material. In general, there is no obligation to record all operations on a digital archive, nor to use systems that automatically produce auditable records. Moreover, this style of record-keeping and preservation does not allow for a quick reading of the item's history.

In the antifraud domain, Circular n. 1-2018 demands a little bit more [33]. The "chain of custody" is a separate document, not included in the report and which in not required by the legal standards of criminal or administrative procedure. It shall list the name of whoever participated in the gathering of the digital material – police agents and defendants alike; it shall contain a precise list of the data

[33] Guardia di Finanza, Circular n. 1-2018, vol. II p. 31.

seized, specifying the type of digital evidence, the hash value, every relocation of the exhibit and the location where it is currently stored.

2. *Investigating authorities*

In the Italian legal system, digital investigations, alike other kind of investigation, may be carried out by law enforcement agents (both in their criminal and administrative law capacity), by computer forensic consultants hired by the prosecution service, or by computer forensic consultants appointed by the judge.

2.1. *Law Enforcement*

No specific provision is established by Italian statutory law to specifically allocate personnel with adequate technical experience for the carrying out of digital investigations.

With regard to the antifraud investigations which are the focus of the present study, the issue is however tackled by a few *Guardia di Finanza* ("GdF") internal Circulars, not all of which are publicly available [34].

In particular, both under an administrative and a criminal law perspective, a major role is played by the already mentioned Circular n. 1-2018 ("*Manuale operativo*"). According to it, in all cases where it can be reasonably foreseen that *Guardia di Finanza* will have to gather digital evidence, personnel with adequate technical knowledge, "although not necessarily officially certified", shall be called to participate to the operation [35].

The Circular does not explicitly differentiate between the two main phases which may be recognized in digital investigations [36], neither as such, nor in the allocation of personnel with different

[34] Guardia di Finanza is the Italian financial police, whose activity ranges from administrative to criminal investigations. A specific list of GdF's tasks may be found at Article 2, Legislative Decree no. 68 of 19 March 2001 and in the Decree of the Minister of Interior of 28 April 2006.

[35] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 28 ff. "partecipazione di personale in possesso di adeguate cognizioni tecniche, ancorché non munito di specifiche qualifiche".

[36] In general terms, Phase one consists in the process of data acquisition, while Phase two concerns the operational analysis of the data acquired in light of its use for the ongoing investigation. For a detailed illustration of the main steps in digital

skills in relation to the specific steps of the investigation. However, the Circular does distinguish two main roles in the expertise of the *Guardia di Finanza* personnel, depending on the complexity of the operation to be carried out.

For operations with a high degree of complexity, the Circular requires the intervention of qualified personnel, specialized in "Computer Forensics and Data Analysis" (hereinafter referred to as "CFDA") [37].

The intervention of the CFDA, as well as the activities carried out and techniques applied by the latter shall be annotated in the report of the operations [38]. CDFAs are professional figures that belong with *Guardia di Finanza* in its territorial headquarters. Their expertise results from the combination of specific education in the field and the successful attendance to special trainings internally organized by the financial police [39]. Where a specific digital investigation demands a centralized intervention, further highly qualified support may be requested also to the centralized GdF *Nucleo Speciale Tutela Privacy e Frodi Tecnologiche*, established in 2001 [40].

Due to the limited availability of such specialized professional figures, CDFAs are not foreseen to be applied to every step of digital investigations. Neither the Circular, nor other available sources though, exhaustively define what should be considered an investigative act of sufficient complexity to trigger the participation of a CDFA.

Only three examples are provided for in this sense in the GdF Circular. The first, rather vague, is the case in which the target of the investigation makes use (*e.g.* in her business capacity) of "complex informatic systems". The second, is where the devices to be accessed belong to multinational groups which may have adopted shared communication and information systems among subsidiaries. The complexity, in this situation, derives from the fact that accessing information concerning one entity could affect also information referring to other entities or to the overall system. The third, and

---

investigations, cf. *infra*, R. Brighi-M. Ferrazzano, *Digital Forensics: Best Practices and Perspectives*, § 5.

[37] See also *supra*, § 1.4.

[38] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 35.

[39] Operational guidelines concerning the use of CDFAs may be found in GdF, Circular no. 300906 of 13 October 2011 (III Reparto), not publicly available.

[40] Cf. *gdf.gov.it/chi-siamo/organizzazione/reparti/reparti-operativi/reparti-speciali.* The body is also the official *Guardia di Finanza* reference contact before the Italian Data Protection Supervisor.

perhaps more interesting example, concerns the case where a criminal proceeding exists in parallel to the administrative one (either due to a double-track system, or not), or where it is likely that the administrative forensic operation will discover elements from which criminal liability may arise.

On the other side, activities which are not considered complex may include, for instance, the creation of a copy or clone, or the printing of information contained in the device at the presence of the accused [41]. For such and other (undefined) basic operations, mostly referred to the so-called Phase 1 of digital investigation [42], the Circular considers it sufficient the intervention of "First Responders", that is "ordinary" *Guardia di Finanza* personnel, trained with basic technical knowledge.

It is to be appreciated, in this sense, that even for "basic" acts, the Circular does not favor the intervention of personnel with a total lack of technical expertise. In particular, it recommends the acquisition of digital evidence be performed together with the calculation of the hash function as much as possible, also when no CFDA is present [43]. In this regard, the Circular reports that the GdF General Command shall launch training activities focused on the ISO/IEC Guidelines 27037 (Guidelines for identification, collection, acquisition, and preservation of digital evidence – Annex A) dedicated to First Responders [44].

On a systemic perspective, however, using the Circular as a legal basis for the performance of digital antifraud investigations reveals important critical aspects.

It being a mere internal document, above all, strongly undermines its effectivity. The soft law nature of the Circular, indeed, does not confer solid grounds to the defence for challenging potential violations of such standards.

The vagueness of the "complexity" criterion, for instance, makes it rather hard for the defendant to advocate – besides for the few given examples – that her case should have been given priority compared to other investigations [45]. Likewise, on the basis of the Circular, the

---

[41] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 29.
[42] Cf. *infra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, § 5.
[43] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 31.
[44] ID., p. 28 ff.
[45] On which see also *supra*, § 1.5.

possibility for the defendant to challenge a potential lack of professional skills of the GdF personnel appears rather inconsistent.

Neither the law, nor the Circular, indeed, confer to the defence the right to be informed of the specific expertise possessed by the GdF agents intervened in her case. When it comes to law enforcement, no legislative requirement is established to certify the skills of the personnel involved in digital investigations, nor any register exists listing which officials own, for instance, the CFDA specific technical expertise.

Naturally, it is always theoretically possible to challenge the reliability of the investigations at trial, also questioning the expertise of who performed specific investigative acts. Nonetheless, in the antifraud matter, no case has been reported so far, in which the lack of subjective expertise referred to one or more agents intervened in the crime scene has resulted in the exclusion of inculpatory evidence [46].

This is also strictly linked to the fact that the Circular, as any other guideline, does not provide for specific sanctions in case such recommendations are violated, nor, consequently, for specific remedies (in general, and especially for the defendant) in case of potential breaches.

2.2. *Digital Forensics Consultants*

The appointment, role and powers of consultants in criminal investigation is, on the other side, traditionally regulated by law, and precisely by the criminal procedure code. For this reason, the following regulation has a broad scope, not specifically referred to antifraud investigations.

Consultants may be appointed by the judge (court expert or *perito*)

[46] Critical cases on the use at trial of digital evidence collected in violation of the best practices - at least to the extent the breach affects the possibility for the defendant to produce an *alibi* - may however be found in other fields of criminal law. Notorious, in this sense, the "Garlasco" affair (murder case), in which an improper police intervention on the defendant's device irremediably altered the authenticity of the data there contained, cf. Trib. Vigevano, 16 March 2010, in *Cass. pen.*, 2012, p. 287 ff., subsequently overruled (on other grounds) after an annulment of the Supreme Court. Among the several comments on the case, see, with a special focus on the theme, L. Marafioti, Digital evidence *e processo penale*, in *Cass. pen.*, 2011, p. 4509 ff.

or by the parties of the proceeding (*consulenti tecnici*), *i.e*. prosecution service and private parties.

In general terms, consultants appointed by the judge shall be chosen from a register of experts (*albo*) that is established for every tribunal and divided into categories [47]. To be included in such register, consultants shall possess the necessary technical competence, as certified by the related professional association, and have a clean criminal record (at least, from offences committed with intent) [48]. Normally, consultants appointed by the prosecution service shall also be chosen among those included in the expert register used by judges – although in this case, the possibility to appoint also experts that do not belong to it, is not excluded by law [49].

When it comes to digital forensic experts, however, the problem is that, to date, no specific criteria have been established to verify, in a harmonized way, the effective professional quality of the consultants included in the *albi* (not even with regard to the need of having obtained a university degree in informatics [50]). Likewise, no shared criteria are currently into place to determine which specific competences should the expert possess to perform certain digital investigative operations.

Regrettably, therefore, digital forensic experts are often appointed by judges and prosecutors on the basis of inconsistent parameters, such as seniority in the registration to the *albo*, and in any case, without substantial obligations to verify the actual expertise of the appointee in relation to the activity to perform.

This does not mean that in Italy qualified registers of digital forensics expert are currently lacking at all. Some registers have been, for instance, established by sectorial associations, such as the *Osservatorio Nazionale Informatica Forense* – ONIF. No obligation, however, exists to prevent public authorities from appointing as consultants also people that did not go through such an accurate selection.

It may happen, therefore, that subjects with little expertise for the specific task assigned may be appointed as computer forensic

---

[47] Forensic medicine, psychiatry, accounting, engineering and related specialties, traffic and road traffic accidents, ballistics, chemistry, analysis and comparison of interpretation and translation handwriting, cf. Article 67 disp. att. c.p.p.

[48] Cf. Article 69 disp. att. c.p.p.

[49] Cf. Article 73 disp. att. c.p.p.

[50] See, in this sense, the data released by ONIF, as reported by R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, § 4.

consultants, without any possibility for the defence to effectively challenge the lack of specific expertise. Of course, the defendant always retains the right to cross-examine the expert at trial, pointing out potential professional lacunas. It remains a fact, however, that when it comes to digital forensics, the traditional safeguard represented by the existence of professional *albi* is exercising a filtering effect even less efficient than in other fields of scientific expertise. This lacuna, which represents a major flaw in the Italian legal system on digital investigations is currently addressed in a legislative proposal inspired by the Dutch system [51]. The chances of this proposal to be approved, however, are currently hardly foreseeable.

When a consultant is appointed by the judge, she shall also comply with the same independency and impartiality requirements established for the judge [52]. In case such requirements are lacking, the parties, including the defendant, may challenge the appointment of the expert, and obtain her substitution. As anticipated, no general rule exists, according to which a similar effect may be obtained where the consultant substantially lacks adequate qualification or expertise.

Consolidated jurisprudence of the Italian Supreme Court (*Corte di cassazione*) establishes that the impartiality and independency requirements provided for the *perito* do not apply to the prosecutorial consultants appointed in the course of pre-trial investigation. In this case, therefore, parties would be prevented from challenging the appointment of the consultant for lack of impartiality [53]. This lacuna appears especially critical with regard to some of the most severe incompatibility causes provided for by the procedural code, and in particular those concerning: Persons addressed by personal security or preventive measures, and subjects

---

[51] Cf. *camera.it/leg18/126?tab=&leg=18&idDocumento=2084&sede=&tipo=*.

[52] Cf. Article 222 c.p.p.

[53] With regard to the *accertamenti tecnici* of Article 359 c.p.p., cf. Cass., Sez. II, 7 June 1995, n. 8489, in *DeJure* (annotated by R. ADORNO, *Sull'incompatibilità del consulente tecnico nominato dal pubblico ministero* ex *artt. 359 c.p.p.*, in *Cass. pen.*, 1997, p. 2151 ff.); Cass., Sez. III, 7 April 2010, no. 24294, *ivi*, n. 247870-01; Cass., Sez. IV, 18 October 2011, n. 44644, in *C.e.d.*, n. 251663 – 01; Cass., Sez. III, 26 April 2017, n. 39512, in *C.e.d.*, n. 271421-01, according to all which the impartiality and independency requirements established for court-appointed consultants (Article 225(3) c.p.p.) cannot apply, by way of analogy, to the consultants appointed by the public prosecutor.

which cannot be summoned as witnesses by law, or have the right to abstain from testifying, or have been summoned as witness or appointed as interpreter for the trial [54]. Authoritative scholars strongly criticize this interpretation of the Supreme Court [55], which however, has so far been constantly restated.

2.2.1. *Digital Forensic Consultants Hired by the Prosecution Service*

Consultants may be appointed by the prosecutor in case: a) an expert is appointed by the judge during the trial or, in the investigation, during the so called *incidente probatorio* (see below, § 2.2.2), or b) to perform technical exams during the investigation.

In the first case, the consultant has the task of challenging or commenting the results of the court-appointed expert in a purely adversarial perspective. The same power is also conferred to private parties (see below, sub § 3.1).

More relevant for the regime of digital investigation is instead the second case, in which two different situations may occur. The consultant may indeed be hired to carry out: 1) technical exams (Article 359 c.p.p.) or 2) technical exams which cannot be later repeated at trial (Article 360 c.p.p.).

The technical exams of Article 359 c.p.p. do not foresee the presence of the defence, and as a rule, do not constitute evidence at trial. Exceptions (applicable to all elements unilaterally collected during the investigation) are the cases where: i) the parties agree on their use as evidence; ii) repeating the exam has become unrepeatable (and this was not foreseeable in advance); or iii) where the consultant is summoned and then cross-examined as witness at trial.

Different is the regime under Article 360 c.p.p. Here, indeed, not only the accused shall be notified of the upcoming technical exams, but she can also appoint a consultant of her own to question the results of the prosecutorial one. In this case, the results of the technical exam are evidence that can be used at trial. To avoid this procedure (in which, as anticipated, the defence is limited in challenging the lack of

---

[54] In these last cases, before the person has testified. Cf., respectively, letters c) and d) of Article 222 c.p.p., as recalled by Article 225 c.p.p.

[55] Cf. R. ADORNO, *Sull'incompatibilità*, cit., p. 2151 ff; V. GREVI, *Libro III. Le prove*, in G. CONSO-V. GREVI (eds.), *Profili del nuovo codice di procedura penale*, Cedam, Padova, 1996, p. 235 f.; R.E. KOSTORIS, *I consulenti tecnici nel processo penale*, Giuffrè, Milano, 1993, p. 227 ff.

impartiality of the prosecutorial consultant), the defendant may timely ask to activate instead a different procedure, in which a consultant is appointed by the court, the so-called *incidente probatorio* (cf. § 2.2.2).

Although relatively more safeguarding, the possibility to carry out digital investigations through the procedure of Article 360 c.p.p. has come up only recently in the criminal matter.

The Italian Supreme Court, indeed, has long affirmed that digital investigation (Phase 1, and the initial part of Phase 2) are not unrepeatable operations, at least when carried out by expert personnel that can avoid the loss of data. It follows, that the procedure of Article 360 c.p.p., designed for unrepeatable examinations, should not come into question [56].

This case-law, however, seems not to consider that – as illustrated above – the defence is often not in the position of knowing the actual level of expertise of the intervening personnel. Arguments proposed by the Court risk therefore to poorly keep pace with the current law in action, especially until rigorous criteria will be established for selecting digital forensics consultants. Under another perspective, this jurisprudence is also heavily criticized by legal scholars, who highlight that at least the cloning of the device should be considered as an unrepeatable act [57].

More recently, the Supreme Court seems to have indirectly opened a window for a potential, at least partial, overruling. In a case from early 2020, indeed, the Court has recognized that the acquisition procedure prescribed by Article 360 c.p.p. was a legitimate modality able to fully guarantee the respect of the defence rights in digital investigations [58].

---

[56] Cf., *e.g.*, Cass., Sez. I, 25 February 2009, n. 11503, in *C.e.d.*, n. 243495 (annotated by E. Aprile, *Le indagini tecnico scientifiche: problematiche giuridiche sulla formazione della prova penale*, in *Cass. pen.*, 2003, p. 4034; F. Novario, *L'attività di accertamento tecnico difensivo disposta su elementi informatici e la sua ripetibilità,* in *Ciberspazio e diritto*, 2011, p. 75; A.E. Ricci, Digital evidence *e irripetibilità delle operazioni acquisitive*, in *Dir. pen. proc.*, 2010, p. 343 ff.). Cf. also Cass., Sez. I, 26 February 2009, n. 11863, in *C.e.d.*, n. 243922; sez. II, 4 June 2015, n. 24998, *ivi*, n. 264286; sez. II, 19 February 2015, no. 8607, *ivi*, n. 263797; sez. II, 1 July 2015, no. 29061, *ivi*, n. 264572.

[57] Cf. S. Aterno, *Acquisizione e analisi della prova informatica*, in P. Tonini (ed.), *La prova scientifica nel processo penale*, Ipsoa, Assago, 2008; see also R. Brighi-M. Ferrazzano, *Digital Forensics*, § 5 affirming that potentially the whole acquisitive phase could be considered unrepeatable.

[58] Cass., sez. VI, 19 February 2020, n. 12094, in *DeJure,* § 2.4 of the *Considerato in diritto*. In the specific case, a procedure was agreed upon, according to which the

2.2.2. *Digital Forensic Consultants Hired by the Judge*

Lastly, consultants may be appointed by the judge.

During the investigation, the court expert may be appointed in the already mentioned *incidente probatorio* (Article 392 c.p.p.). This procedure represents an exceptional anticipation of a trial hearing, in which evidence is collected following adversarial principles (mainly, cross-examination). It is therefore a procedure which ensures a very high level of protection to the defendant's rights. For this reason, information collected during the *incidente probatorio,* although occurred before the judge entitled to supervise pre-trial investigations, can be used as evidence at trial. The *incidente probatorio* may be activated at the request of the prosecutor or of the defendant in a series of cases peremptorily established by the law. Concerning technical exams, and, potentially, digital evidence, this procedure may be requested in case the information to be collected relates to a person, thing or place whose condition is subject to unavoidable modification [59]; or where the expert exam is deemed to be time-consuming (*i.e.* it could result in a suspension of more than sixty days if carried out during the trial) [60].

Again, therefore, the possibility to trigger the *incidente probatorio* is mostly related to the possibility of defining digital forensics investigation (or certain phases of it) as unrepeatable. Although certainly not common as yet, the application of the *incidente probatorio* procedure with regard to the collection of digital evidence is starting to be reported in criminal proceedings, especially with regard to the controversial investigative step in which a selection of the data relevant to the trial shall be made [61].

The activation of the *incidente probatorio* may pass also through the *accertamenti tecnici irripetibili* of Article 360 c.p.p., at least to a certain extent. According to § 4 of the latter provision, indeed, during the performance of the *accertamenti*, the defendant may request an *incidente probatorio*. In principle, this request should bring to the suspension of the *accertamenti tecnici*. The prosecutor,

---

device was immediately cloned, and the prosecutor's consultant was given 7 days to select relevant material through the use of keywords. The original forensic copy was to be given back to the respective owners.

[59] Cf. Article 392(1)(f) c.p.p.

[60] Cf. Article 392(2) c.p.p.

[61] Cf. R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, note n. 48. See also widely § 5, on the ever-lasting conflict between privacy rights and the need for digital forensics expert to collect complete data to perform meaningful analysis.

however, retains discretion in assessing whether the deferral of the *accertamento* may cause the examination to be no longer usefully carried out. If that is the case, the prosecutor is allowed to proceed in the forms of Article 360 c.p.p. Given the high discretion of such decision, especially in case of extremely volatile evidence such as digital data, it is not so far-fetched to reckon that the possibilities to activate the *incidente probatorio* in this way appear relatively small.

3. *Defence Rights: Information and Right to be Heard*

In the Italian legal system, no specific information right is provided for with regard to digital evidence. In digital forensics investigations (Phase 1 and Phase 2), therefore, defendants enjoy the information rights generally provided for in criminal proceedings established by the criminal procedure code, as amended in light of Directive 2012/13/EU.

This is the case also in the (few) occasions in which the Italian legislation makes explicit reference to the digital dimension in regulating investigative techniques: Here information rights apply that have generally been developed with regard to premises [62].

When digital searches (Article 247 § 1-*bis* c.p.p.) are to be performed, for instance, the accused shall be informed of her right to be assisted by a trusted person (*e.g.* a lawyer), provided that this person is readily available. Such an information shall be contained in the prosecutorial decree authorizing the search, which shall also be delivered to the accused, if present, and to those who have the momentaneous availability of the place (or of the device, could be argued) [63].

Similar consideration applies also to inspections (Article 244 ff. c.p.p.), even though in this case safeguards (rather incoherently [64]) differ from those of searches. For what is here more relevant, in

---

[62] For a general recognition of the Italian legislation concerning investigative techniques after the entry into force of the Budapest Convention, see, for all, S. Aterno, *Le investigazioni informatiche e l'acquisizione della prova digitale*, in *Giur. merito*, 2013, p. 955 ff.; L. Lupária (a cura di), *Sistema penale e criminalità informatica*, Giuffrè, Milano, 2009; A. Vitale, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. Internet*, 2008, p. 509 ff. Cf. *supra*, § 1.2, also for a reference to seizure (Article 254 *bis* c.p.p.).

[63] Cf. also Article 250 c.p.p.

[64] Cf., for all, A. Camon, *I mezzi di ricerca della prova*, cit., p. 358.

particular, also before performing (digital) inspections, the prosecutorial decree shall be delivered to the accused and to those who have the momentaneous availability of the place (or of the device), if present. No specific provision, however, can be found in this regard concerning a duty to inform the accused of her right to be assisted by a trusted person or a lawyer. [65]

More tailored provisions are contained, on the other side, in the 2018 *Guardia di Finanza* Circular: The accused is required to sign (along with GdF agents) the clones of the devices and documents acquired by the First Respondents, as well as the printing of those data considered of main interests. This is necessary in order to produce an authenticated copy. The accused has also the right to request a clone of the working copy. As already argued, however, these (scarce) requirements find their legal basis only on soft law, so no remedy is recognized in case of their violation [66].

From the above, it emerges that, in the Italian legal system, the accused enjoys certain general information rights, and can, at least in case of searches, count on the presence of a trusted person.

Contrary to what occurs in OLAF's proceedings [67], however, the accused has no right to be informed neither of the specific procedures that will be followed by the investigating authorities in acquiring the data, nor of what use will be made of such data; nor, lastly, of which safeguards will be applied to its retention; or for how long such data will be retained.

This limitations in the information rights are mirrored in an uncertain regulation concerning the degree of the defendant's participation to digital forensics investigations. As previously illustrated (§ 3.1), indeed, under criminal procedure law it is still debated which legal participation mechanism should apply in order

---

[65] The provisions referred to searches and inspections apply also when the latter are carried out by law enforcement, cf. Articles 352 and 354 c.p.p. The lack of information rights in this regard is only partially mitigated by Article 366 c.p.p., according to which, when the defendant's lawyer has not been pre-warned of the upcoming investigative measure, the reports of the investigative acts carried out shall be made available to her within three days from their performance. This deadline may however be postponed by the prosecutor with a reasoned decree, on the basis of serious ground. The decree may be challenged by the defendant before the judge supervising the investigation phase.

[66] Guardia di Finanza, Circular n. 1-2018, vol. II, p. 28 and 30. Cf. *supra*, § 2.1.

[67] For a description of the OLAF Guidelines, see R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, § 3.3.

to substantially safeguard to the defence rights (Article 359, 360 or 392 c.p.p.).

A few more provisions on this matter may be found also in the *Guardia di finanza* Circular. According to it, Phase 1 shall be performed by GdF at the presence and with the assistance – where existing and possible – of the specialized (IT) personnel of the accused's company (as the Circular mostly refers to cases of accused which are owners of a business enterprise) [68]. The assistance of such personnel is especially recommended during the identification phase. If no such personnel exists or is available, *Guardia di finanza* shall ask the accused to be assisted by a trusted person – who may also be a lawyer [69].

3.1. *Defensive Investigations*

The defendant has the right to appoint her own consultant in all cases in which a consultant is appointed a) by the judge, during the trial (*perizia*, Articles 220 ff c.p.p.) or during an *incidente probatorio* (Article 392 c.p.p.), or b) by the prosecutor during the investigation, in case unrepeatable exams shall be performed (*accertamenti tecnici non ripetibili*, Article 360 c.p.p.).

In these circumstances, the consultant of the accused has the power to challenge the results of the other experts, and formulate her own assessment on the matter to be submitted before the court.

Since 2000, the defence lawyer is also entitled to carry out her own defensive investigation (Article 391-*bis* ff. c.p.p.), regardless of the prosecutorial activity [70]. Especially where the digital devices or data are already in the availability of the defendant, this power is often used to perform technical assessment, through the appointment of an expert consultant (cf. also Article 233 c.p.p.).

The results of defensive investigation have – at least theoretically – the same evidentiary value of the elements collected by the prosecutor during the investigation [71]: Normally, all the information

---

[68] ID., p. 28.

[69] ID., p. 29.

[70] As established by Article 11, Law 7 December 2000, n. 397.

[71] The relatively recent establishment of the accusatorial model in Italy, however, still offers the ground to some more inquisitorial-oriented interpretations of the defensive prerogatives: Although not often officially expressed, judges which tend to consider unreliable the results of defensive investigations just because they come

collected in the pre-trial phase cannot be used as evidence at trial, but only by the parties to develop their own procedural strategy. As (a quite broad) exception, however, such information may become evidence: For instance, in case of documents, or where the acquisition of such elements cannot be replicated before the court [72].

For what is more relevant to the present study, in particular, Article 391-*sexies* c.p.p. ff confer the defendant the possibility to access to locations (also private, with the consent of the owner, or after judicial authorization), and to carry out examinations of "objects". The latter, in lack of any further specification, could be interpreted as including also digital devices.

If, already before its performance, the exam is considered unrepeatable, the defence lawyer cannot autonomously proceed (Article 391-*decies* c.p.p.). She shall instead previously inform the public prosecutor, in order to allow the latter to exercise its prerogatives under Article 360 c.p.p. (see above), or in any case, to allow the latter to assist to the exam.

3.2. *Consent of the Accused*

The consent of the accused is only partially valued in the criminal procedure code: It merely establishes that a search may be avoided if the person consents to produce the requested document or piece of information (Article 248 c.p.p.).

When it comes to digital investigations, a few further (and not binding) provisions may be found in the *Guardia di Finanza* Circular. There, the consent of the accused may become relevant on several occasions, influencing the procedure that GdF shall carry out to perform digital investigations.

Firstly, the person may give her consent "lending" her facilities and personnel to support the operation of the *Guardia di Finanza*. If such cooperation is denied, the refusal shall be annotated in the report of the procedure. This has the effect of preventing GdF from carrying out digital investigation directly in the facilities of the

---

from the defendant side are not a phenomenon unheard of. For a few examples, see Cass., Sez. III, 18 February 2020, n. 16458, in *Sistema penale,* 28 September 2020 (with observations by R.E. KOSTORIS, *Una grave mistificazione inquisitoria: la pretesa fede privilegiata del responso del consulente tecnico dell'accusa*), and Cass., Sez. II, 24 September 2014, n. 42937, in *DeJure*.

[72] Cf., for the elements collected by the defence, Article 391-*decies* (1) and (2) c.p.p.

accused: Such activity shall instead be performed in other locations. That means that *Guardia di Finanza* is entitled to apply all the necessary measures to successfully carry out such operations elsewhere (such as the cloning of the device, and the creation of backup copies) [73].

Secondly, according to the Circular, the consent of the accused is relevant in case of digital evidence stored on the cloud.

If the investigators deem it necessary to access to information stored on the cloud from a computer located in the premises to be inspected, *Guardia di Finanza* shall immediately ask for the cooperation of the accused. In case she refuses to do so, and where the cloud is referred to the subject as a private person (and not in her business capacity) the lack of consensus triggers the need for the GdF to obtain a judicial authorization before accessing cloud data [74].

3.3. *Remedies*

Given the lack of specific, and above all, binding rules concerning the acquisition of digital data, no *ad hoc* remedies are provided for in the Italian legal systems against violations of technical standards. This lacuna is especially critical with regard to breaches of the best practices caused by negligence or lack of sufficient expertise in the intervening law-enforcement personnel, when the data acquisition has been carried out unilaterally. In this case, indeed, the defendant may not only be prevented to access the data, but even to properly understand in which stage of the digital investigation the mistake has occurred, and why.

Against the lack of specific remedies, parties to the proceeding can complain about the violations occurred (also) in digital investigations using the ordinary appeal remedies (judicial review before the Court of Appeals and before the Supreme Court – in the last case, only on the basis of legitimacy grounds, cf. Article 606 c.p.p.).

Moreover, when it comes to searches (also digital searches), a further remedy may be activated. This possibility however depends on whether the search is followed or not by a seizure (of the device and/or of the digital evidence).

---

[73] Cf. also Guardia di Finanza, Circular n. 1-2018, vol. II, p. 28-29. This case founds its legal basis also on Article 52(7) and (9), D.P.R. no. 633/1972.

[74] Id., p. 33; cf. also Article 52(3), d.P.R. n. 633/1972.

Only in the first case, the accused may challenge the opportunity and legitimacy of the seizure, as well as potential errors related to the search procedure, through a specific remedy that may be activated just after the performance of search, called *riesame* (Article 257 ff. c.p.p.) [75].

On the contrary, in the second case (where a search is carried out, but no seizure derives from it), the Italian legal system does not provide for any specific remedy that can be immediately activated. Perhaps partially related to the lack of a formal recognition in the Constitution of the right to privacy, but certainly totally unacceptable for a system that truly wants to comply with the rule of law principle [76], this lacuna has already been sanctioned by the European Court on Human Rights (in cases not related to digital evidence) [77].

3.4. *Third-Party Rights*

Lastly, in case of (digital) search, also rights of third parties found some recognition in the criminal procedure code. Also in this context, however, a distinction shall be made, here between third parties which own the seized device(s) or the seized data, and those who do not.

Like defendants, the first may challenge the seizure of their device through the remedy of *riesame,* already illustrated.

On the other hand, for the second category of subjects – who have interests in the information seized, but cannot officially claim an ownership on the latter – no specific remedy is established by law. The aforementioned 2017 Supreme Court *Andreucci* decision could perhaps be used to try at widening the level of protection also for third parties in this regard: However, the intervention of the legislation certainly seems mostly appropriate [78].

---

[75] And, specifically, within 10 days from its enforcement or as of the different date when the person concerned was informed of the seizure. As anticipated, in a 2017 case, the Supreme Court clarified that the request for *riesame* may be issued both with regard to the device, and to the digital data (*i.e.,* also to request the production of the device containing the clones of the data, once the original device had already been returned to its owner), cf. Cass., Sez. Un., 20 July 2017, n. 40963, in *C.e.d.*, n. 270497-01 on which see *supra*, note 12.

[76] On which, if you wish, G. LASAGNI, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *NJECL*, vol 9 (2018), i. 3, p. 386 ff.

[77] Cf. ECtHR, 27 September 2018, Brazzi v. Italy.

[78] Cf. *supra*, note 12.

Similarly to the case of the defendant, no specific remedy is provided for in case of searches not followed by seizure.

4. *Digital evidence at trial*

4.1. *Admissibility*

In the Italian criminal justice system, the trial is conceived as completely separate from the investigation. The judge largely ignores what happened during the preliminary investigation: the trial dossier, at the beginning of this phase, can only contain a limited set of documents listed in art. 431 c.p.p., among which the reports of non-repeatable acts such as inspections, searches, seizures and non-repeatable ascertainments. In general, the parties can agree on other pieces of evidence they want to insert in the trial dossier.

Every other piece of evidence – expert testimony, further analysis and so on – has to be gathered anew in front of both parties and the trial judge, to fully ensure the adversarial character of the procedure.

The lifespan of a piece of evidence at trial is therefore divided in three phases: admission, gathering and evaluation.

The admission phase is placed at the beginning of the trial. The parties shall name all witnesses they intend to have examined (including the expert consultant) and file their list within 7 days from the first hearing. At the first hearing, all parties shall present their evidentiary request to the judge, that shall rule on admissibility. At this stage, the judge can exclude only manifestly superfluous or irrelevant evidence [79].

At any stage of the procedure, the judge shall exclude all evidence that has been gathered in violation of the prohibitions set by law. So, the violation of a procedural rule does not automatically entail the exclusion of a piece of evidence: the law must specifically forbid a certain option to trigger the exclusionary rule, but if the law simply lays down a path, the non-observance is not sanctioned [80].

---

[79] For a general overview on the Italian system and specific problems with the admissibility of OLAF reports as evidence, see M. Caianiello-G. Lasagni, *Italy*, in F. Giuffrida-K. Ligeti (eds.), *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, University of Luxemburg, Luxemburg, 2019, available at *orbilu.uni.lu*.

[80] At least, not with the exclusion of the collected piece of evidence. The agent misapplying the rules, however, could be disciplined since every official is bound to observe all procedural rules, despite the effects on the trial.

This setting also applies to digital evidence: for example, the law prohibits to perform a non-repeatable ascertainment without giving notice to the opposite party, and if the prosecutor, for example, proceeded without warning the defense beforehand, the ascertainment should be excluded. However, the law states that the police have to gather evidence with techniques that ensure the integrity of the original, but does not explicitly prohibit inadequate techniques. The police, therefore, can freely choose how to proceed, and even if it is impossible to ascertain whether or not the original has been manipulated, it will not be excluded.

The code of criminal procedure does not provide for an exclusionary rule in case of breach of the chain of custody. The evidence can be used at trial and has to be evaluated by the judge. The best option for the interested party, at this point, is to question its reliability and persuade the judge that the digital material cannot be trusted.

Of course, potential threats to authenticity could emerge from a full record regarding the item: the gathering, the preservation, the analysis, the interpretation should be thoroughly reported in order to allow for persuasive objections. However, the legislation does not seem to require the level of detail that would facilitate this operation.

The interested party can challenge the credibility of that piece of evidence, and it is her burden to prove that the reliability of the item has been compromised. It is not upon the party asking for the admission of the item to show that the piece of evidence is what she claims it is.

4.2. *Production of evidence in different proceedings*

During an administrative investigation, the authorities have the duty to warn the prosecutor whenever the facts they ascertain could be qualified as a crime. Moreover, if the agents realize that the alleged administrative infraction could be construed as a crime, they shall proceed according to the rules of the code of criminal procedure (art. 220 disp. att. c.p.p.). The duty applies from the moment in which it is clear that the infraction could lead to criminal responsibility.

The administrative complaint is admissible as evidence as a document (art. 234 c.p.p.); the judge can always use for her decision the part of the complaint that was drafted before the elements of a crime surfaced. The part drafted after that moment can only be used by the criminal judge if the rules of the code of criminal procedure

were duly observed. The suspect of a criminal investigation, in facts, enjoys rights that would not be necessarily granted in an administrative proceeding; therefore, the criminal trial can only consider as evidence what was gathered abiding by standard safeguards.

In theory, the system protects the taxpayer/suspect from a label trap; in practice, however, the line is a thin one to walk [81]. It can be hard to identify the precise moment when the administrative infraction may be understood as a criminal offence, and the investigators themselves could basically decide when to trigger the responsibility to act according to the code of criminal procedure. In a recent case, for instance, the police were conducting an administrative investigation; they decided to talk to the taxpayer first, and to check the volume of non-declared income later. The nature of that infraction – criminal or administrative – depended on the amount of undisclosed revenues: the police could not have known whether they were investigating a crime or not, because they decided to ascertain the sum only after the interviews, even though they should have known that the fact they were investigating was potentially a crime. The Court of cassation did not exclude the administrative complaint from evidence, affirming that the duty to apply the code of criminal procedure is only triggered when all elements of a crime have surfaced, not before [82]. The prosecution was not required to show that the police acted in good faith.

The evidence gathered during a criminal trial can be used as evidence in another criminal trial. Non-repeatable evidence can transit to another proceeding, as long as the non-repeatable character of the ascertainment was not foreseeable. If the evidence was given in form of statement (*e.g.*: expert testimony), it can be used in another trial only if the defense lawyer participated was present at its gathering, or with the consent of the accused.

[81] On this point, see M. Busetto, *Utilizzabilità delle prove tributarie nell'ambito del processo penale*, in *Leg. pen.* (*web*), 28 March 2020.

[82] Cass., sez. III, 4 June 2019, n. 31223, in *C.e.d.*, n. 276679-01.