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 *

ANTIFRAUD INVESTIGATION AND DIGITAL FORENSICS: A COMPARATIVE PERSPECTIVE

1. *Introductory remarks*

The point of all procedures is to harness state authority, to assign it terms and conditions to prosecute infraction without crashing individual liberties. The current solutions reflect an equilibrium that has always been dynamic: the understanding of state power develops overtime, and so does the compass of liberties; the optimum needs constant updating, or the balance would shift one way or another. However, the change that the digital revolution has brought about is so deep that tweaking the system could not be enough. Both plates of the scale have been somewhat transformed in quality and quantity: citizens have more and more diverse opportunities, but the state has the capacity to interfere with civil liberties in a much deeper, and yet less detectable manner. Moreover, the normal investigative process has to be conjugated with technical rules, to ensure the authenticity of evidence and the reliability of the information that the item can deliver.

---

* 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, 2, 3, 8 and 9, and G. Lasagni is the author of §§ 4, 5, 6 and 7.

This essay compares the complex reshaping of procedures occurred in Germany, Italy, Luxembourg, Spain and the Netherlands. In doing so, it will not delve too much into details: the previous papers have already analyzed each legal system in great depth [1]. The aim of this contribution is not that of repeating how different countries regulate digital investigations; it is that of highlighting similarities and – more interestingly – differences in general approach: what overarching principle have been effective in counterbalancing state power? What fundamental flaws do the current legislative arrangements show?

In answering these questions, we will provide a critical assessment of the *status quo*, laying the ground for innovative solutions that will be summarized in the concluding remarks.

Our main focus will be on searches and seizures, that constitute the main funnel for digital evidence into criminal and administrative proceedings. Normally, the criminal regulation is the most exhaustive and pervasive; we will therefore point out the differences with the administrative proceeding only when necessary.

2. *Constitutional and regulatory framework*

Looking just at the different constitutional texts, the innovation would go unnoticed. All the involved countries have rigid constitutions and none of them bothered to formally amend the text. Nonetheless, it does not mean that no change has occurred at that level: most of the concerned countries (Italy, Luxembourg, the Netherlands) resorted to super-national sources to bestow new rights upon the citizens – namely, the right to privacy – or to better define the limits of state interference through the principle of proportionality. Although with different styles and different results, the three countries show a similar use of the ECHR (especially art. 8) and of the CFREU, that are invoked in court to

[1] Especially when it comes to Germany, Italy, Luxembourg and Spain, every mention has been based on the other contributions to this book: see *supra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*; L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy;* S. GLESS-T- WAHL, *The handling of digital evidence in Germany*; K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*. They will be specifically referred to only when necessary, but they constitute the basis for every claim and example mentioned in this chapter.

set aside (Luxembourg, the Netherlands) or to interpret (Italy) national rules [2].

Germany and Spain have shown to rely more on internal sources, for different reasons. In Germany, the Federal Constitutional Court has been famously active in interpreting the provisions and creating new fundamental rights: privacy has been acknowledged and protected since 1983, and the Court has recently affirmed the right to a confidential use of an informatic system. The proportionality principle is a cardinal rule of German constitutional law: extrapolated from several provisions of the Grundgesetz, it is a veritable guide for the Federal Constitutional Court when it comes to setting limits to new forms of state interference.

The Spanish legal system reaches similar results with a partially different approach. The Spanish constitution is relatively young: it entered into force in 1978 and it directly contemplates privacy as a fundamental right (art. 18), also in connection to human dignity and the free development of personality granted by art. 10. Therefore, there has been no need to forge a protection out of preexisting statements, or to apply art. 8 ECHR in some form. As for proportionality of state action, it is also considered an underlying principle since a landmark decision of the Spanish Constitutional Court dating back to 1996.

These constitutional yardsticks should shape the legal response to every stage of the digital investigation: criminal and administrative proceedings should be regulated in order to allow an effective prosecution, while infringing upon privacy as little as possible, only if it is necessary and when circumstances justify the entrenchment.

On the legislative level, four over five of the considered countries (Germany, Italy, Luxembourg, the Netherlands) have just extended the rules on ordinary searches and seizure to search of a mass storage device and the seizure of digitally stored information: hence, the law does not provide for specific, additional requirements [3]. The measures, after all, were conceived exactly to strike a balance: in the

[2] In Italy, only the Constitutional Court can declare the prevalence of ECHR on a given provision. Ordinary courts can only interpret the provisions in force in the light of the Convention.

[3] The authority that can trigger the measure varies according to each legal system. It can be carried out by the investigating judge, the prosecutor or the judicial police in Luxembourg and the Netherlands; by the prosecutor or the judicial police, without previous judicial authorization in Italy; by the prosecutor or the judicial police, upon the authorization of the investigating judge in Germany. For a

physical world, the authorities can look for something and take only what is recognized as relevant to the investigation; the search itself is instrumental to the proportionality of the seizure. Applying this framework to data, though, has not proven as effective: a single mass-storage device normally contains a large amount of data; going through all of it on the spot is almost impossible, and the operation would raise a number of technical issues that the legal texts just marginally envisage.

First of all, the relevant data could be encrypted or simply well hidden in the mass of information, and a search on the spot could miss the needle in the haystack. Second, all operations on the device could compromise the integrity of the dataset, making further analysis unreliable or even impossible [4].

It is worth stressing the point again: legal provisions do not contemplate these difficulties, for they have been tailored for a traditional, physical investigation. Hence, practitioners have adopted either working agreements (Germany, the Netherlands), either guidelines (Italian *Guardia di Finanza*) to deal with some of the extra steps that data require.

The traditional sequence – search first, and then seize what is relevant – survives, but only for trivial cases, where there should be no need for complex analysis (Italy). For example, if the law enforcement authorities should search for a single transaction record, they could just go through the archive, find the one thing they need, print it out and seize it. This way of proceeding, however, can raise serious issues as the operation gets more complex. The simple act of searching what is relevant can alter or destroy data, compromising the data set. Therefore, the acknowledged best practice does not favor this solution. On the contrary, it demands the seizure of the device or, if the circumstances allow for it, the mirror-imaging of the entire memory directly on the spot. The idea is to duplicate the original collection of information in order to preserve it; all analysis should be conducted on a second, working copy to ensure the protect the original and ensure the repeatability of all operations.

From a technical standpoint, the procedure constitutes the best

---

breakdown on how the examined Member States dealt with the different procedural rights in digital investigation, see below, § 6.

[4] For more details, see *supra*, R. BRIGHI-M. FERRAZZANO, *Digital forensics: best practices and perspectives*.

available option; however, form the legal point of view, it generates three difficulties [5].

The first one concerns the relationship between the device and the data. From the investigator's perspective, they often have the same evidence to offer: the hardware itself is rarely interesting per se, it becomes useful as a container of information. Therefore, it is often suggested not to seize the device: copying the entire memory on the spot should suffice; or to physically impound the hardware for the time that it takes to make a copy. The solution should be dictated by the proportionality principle itself: holding onto the device longer than necessary would be a gratuitous encroachment on the liberties of the subject. Moreover, when it comes to the right to judicial review, the copy should tantamount the hardware's seizure: data are effectively taken and kept for the records despite the hardware has been returned. In Italy, unlike all other countries involved in the research, this equivalence has not yet been fully established.

The second point deals with the amount of information that the best practices require to gather. Taking everything first is inherently disproportionate and should make a selection necessary: a single mass-storage unit could contain a mishmash of data ranging from the accounting records to the holiday photo-album of its owner.

Third, these legal systems recognize a strong protection of communications. Content data are normally protected by strict requirements and time limits; however, when it comes to seizing emails or other stored communication data, none of these protections apply (the point was explicitly addressed for Germany and Italy).

This legal model, as mention above, is adopted by four out of five of the concerned countries, whereas the Spanish legal system has adopted a different style, that successfully tackles two of the aforementioned issues. Instead of extending the rules on searches and seizures, the Spanish legislature passed a sweeping reform in 2015, introducing a new chapter to the Ley de Enjuiciamento Criminal (LECRIM). It contains common principles as well as precise rules for all investigative measures that technology has made available: interception of communications, eavesdropping, GPS tracking, video surveillance, covert online searches and gathering of stored data have been put in the same macro-category. There is no distinction between communicative data and non-communicative

[5] For a more considerate, technical proposal, see R. Brighi-M. Ferrazzano, *Digital forensics,* cit., § 7.

data; all the techniques put the proportionality principle in serious danger, therefore they all have to abide by the same basic principles and requirements. All the invasive techniques regulated by that chapter – including the search and seizure of mass storage devices – must respect the principles of specialization, adequacy, exceptionality, necessity and proportionality (art. 588 bis a § 1 LECRIM). Moreover, the meaning of proportionality is further illustrated by art. 588 bis a, § 5 LECRIM: the investigative action is proportionate when the sacrifice of the affected rights and interests does not surpass the benefit for third parties and for the public interest. The latter is to be measured according to the severity of the fact, its social significance, the intensity of existing evidence and the relevance of the expected result.

In order to search and seize a mass storage device, the prosecutor needs a previous judicial authorization that must specify the conditions and the scope of the search. In case of urgency, the police may extend the search to devices that were not mentioned in the warrant, but they have to inform the judge immediately or within twenty-four hours. The court has to issue a reasoned decision within seventy-two, with which it can uphold or revoke the action.

This setting seems to find a suitable answer to some of the questions that the "traditional" model leaves open. The system has leveled the protection of all kinds of data, and it closes the communication loophole: the procedure to acquire content data is the same as the procedure to search and seize a mass-storage device, therefore the protection does not degrade according to the techniques that the prosecution decides to adopt.

Moreover, the law does clearly and consistently stress the need for a proportionate action. Beyond the general provision, the LECRIM details more facets. For instance, it expressly states that, unless the measure can be justified, the hardware should not be seized when it would cause serious damage to the owner and it would be possible to secure data by copying them (art. 588 sexies c § 2). The Italian legal system has a similar rule, but its scope is subjectively limited to service providers and providers of computer, electronic and telecommunication services (art. 254-bis c.p.p.). The Spanish version seems more adequate. When the law enforcement authorities do not have a specific reason to retain the hardware, the use that the device serves should not matter: police should avoid the seizure for it would cause unnecessary damage to the individual.

This legislative order, not being an adaptation, is more successful in establishing procedural safeguards. However, a big conundrum

remains, no matter how advanced the legislative framework. The technical standards – precisely spelt out in Spain, as we are about to see – recommend the collection of the full data set, whereas the legal imperative should be "the least, the better". Especially for cases that need a forensic analysis, the collision between the two golden rules seems inevitable, and the clash becomes particularly problematic when privileged information is involved. All legal system set up more procedural requirements and stress the proportionality principle even more; however, the forensic optimum remains the copying of the memory and sieve out the relevant material after a careful and sound analysis.

Choosing beforehand, on the spot, is impossible or not recommendable; the gathered data must therefore be analyzed, interpreted and selected for trial. These steps are crucial, but all concerned legal systems focus exclusively on the measures aimed at gathering the digitally stored information; there are no legal yardsticks for the analysis of the material and the interpretation of the results. Moreover, if the stress on authenticity brought about a certain awareness on the most reliable copying techniques, the question on how to examine the material has not had the same success so far.

Once again, soft law may play a major role: in Spain, for example, the national agency for standardization UNE (Una Norma Española) has issued a full set of specific guidelines [6]. They are largely based on ISO and ENFSI standards, that are internationally regarded as the blueprint for every best-practice. The Spanish police is normally running the analysis in-house, and they apply the UNE rules at all stages of the digital investigation. Regarding analysis, the guidelines provide for a detailed, but not exhaustive list of operations that the investigators should perform: this indication serves as a checklist that helps establishing an epistemological baseline for all parties involved. For instance, it could be easier for the defense attorney to convince the court that the analysis is partial or unsound, if he can clearly show that the analyst leapfrogged through the list and omitted some crucial operations.

No other country, however, has such a clear landscape on soft law, technical standards and analysis, and that is not because of lack of existing, authoritative best practices. Spain has just decided to

[6] See *supra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 3.1.

elaborate its own through a national institution, but the international scene offers multiple options: from ISO/IEC standards to OLAF guidelines. Nonetheless, Germany and the Netherlands' prosecution offices work on internal agreements that are not available to the public, or on regional directives. Italian *Guardia di Finanza's* guidelines are not universally adopted, are mostly ignored by courts and remain silent about analysis.

Thus, the responsibility of the analysis rests on the shoulders of the subject that performs it: often a trained member of the police (Germany, Italy, Luxembourg, the Netherlands) or an expert consultant. She is alone in deciding what to look at, how to proceed, what analysis to perform and how to interpret the results. On the one hand, the strategy makes sense: if someone has been specifically trained to deal with that type of evidence, one could assume that the item is in safe hands [7]. On the other hand, the expert's work could be easier to attack, support or assess if it could be measured against a background of common practices, recognized by all concerned parties.

Despite the absence of a clear shared strategy, all reports emphasize the use of search engines to go through the material. The software allows for targeted queries based on keywords: the system will highlight the hits, id est the files that respond to a given keyword. This tool speeds up operations considerably, especially when the experts need to analyze multiple devices. Moreover, it is a valuable means for protecting the privacy of the individual and making sure that the investigation has a limited scope: the system will scrutinize material according to relevant, preselected inputs and will not devolve into a fishing expedition. Besides, search engines are often adopted due to time and resources constraints: each investigation could potentially bring in new devices to analyze, if the specialized units had to manually go through every file, they would be swamped.

Search engines seem to offer a good balance, as they seem to offer a better protection of the individual's liberties, a better use of resources within police departments and inherently reduces the scope of the search to a definite number of pre-selected keywords. However, the case law shows new issues arising from the use of the tool: in Luxembourg, the police shared a list of keywords with the defense

[7] For more details on digital forensic experts and first responders, see *infra*, § 6.2.

before the selection but used different inputs for the analysis. According to the defense, the change had excessively broadened the scope of the search, but the Court of Appeal established that the investigating judge is free to select whatever keywords she deems appropriate to find out the truth.

The last step of the analysis should be the interpretation of the results: the expert has to put her findings into context and reach a working conclusion. For instance, the same file, named "Client list 2020", could assume a certain meaning if it were found on the desktop, but it could mean something else or if it were found in an encrypted folder named "Off-the-books accounting".

This step does not overlap with the judicial evaluation of evidence: the international standards provide for criteria aimed at helping experts in this final step. On the national level, however, only Spain deals with the issue through the UNE guidelines: they offer a series of suggestions in order to make sure that the findings take the full context into account.

After analyzing all gathered data, the investigators should be able to discern what is relevant from what is not: normally, the relevant information is mixed with files that should remain private and have no place in a trial dossier. The law, as mentioned, does not regulate this scenario, and the courts had to come up with selection mechanisms. For instance, Luxembourgish courts established a procedure articulated in three steps: the seizure of the device or the copy of the entire memory; the selection of relevant information and, last, a new seizure, limited to the relevant material.

The German courts have opted for a similar style: in one case, 14 million files were seized (through copy); the police selected just 1.100 file as relevant. A copy of the full set of data was preserved for the records, while the 1.100 relevant documents were printed out and presented at trial [8].

In Italy, there is no selection procedure in place. In practice, the relevant files are printed out and added to the trial dossier because of time constraints, but a full copy is also normally attached. The courts are sometimes showing more sensitivity to privacy issues, but there is still no precise guideline in place.

[8] ECHR, 25 July 2019, Rook v. Germany.

3. *Copyright issues*

None of the examined legal systems impose the obligation to gather and process data through open source, freely available software. As a result, investigators and consultants can use proprietary programs, which can raise two sets of issues related to the reliability of the analysis and the accessibility of the results.

The first complication is not exclusive to digital evidence: in 2017, a federal judge of the Southern District of New York ordered the New York City's crime lab to disclose a disputed, proprietary software that was used to establish the likelihood that a specific DNA profile was present in a mixed sample [9]. The source code was released and analyzed, its reliability was seriously questioned: the method was discontinued, and the State's Supreme Court had to call for the re-examination of all cases where it had been used [10]. The more the volume of digital evidence to analyze increases, the more investigators will rely on off-the-shelf, proprietary software that can automatically execute most of the tasks. It is cost effective, and it could allow to train less people: if the tool is mostly autonomous and user-friendly, specific qualification is not essential. So far, the egregious example of New York City's lab has not found a parallel in the domain of digital forensics, but it could nonetheless serve as a cautionary tale: software is not infallible, and it is good to keep a critical eye on it [11].

The second hurdle concerns interoperability. Processing data with a licensed program may make it more difficult to read the results of process the data anew, if one does not have a version of the same program at the ready. The problem deepens when the software is only available to the police or has been developed in-house and is not available on the market: in such a situation, the defense could control the analysis only by repeating it entirely, if a copy of the original has been preserved for the record, probably with a different software. Even if the program was available on the market, there could be an affordability issue: what if the tool is too expensive for the defendant to buy? Should the state acquire a copy for the

---

[9] See L. KIRCHNER, *ProPublica Seeks Source Code for New York City's Disputed DNA Software*, in *propublica.org*, 25 September 2017.

[10] New York Supreme Court, 25 September 2019, State of New York vs. Thompson, in *nycourts.gov*.

[11] See *supra*, R. BRIGHI-M. FERRAZZANO, *Digital forensics*, cit., § 6 for the best practices regarding the equipment and the upkeeping of a digital forensic laboratory.

accused? These questions were addressed by the European Court of Human Rights [12]: the German police seized 14 million electronic files from a variety of devices that got seized, copied by mirror imaging and given back to the legitimate owners. Every copy could have been read with a program that was available "free of charge" (the ECtHR does not specify whether it was an open-source software or not). However, the police analyzed all the material through a trademarked software, and the results were readable only through that program. The license was available on the market for € 4.031,72. At the end of the analysis, 1.100 files were considered relevant for the criminal proceeding, printed out and included in the paper dossier, which was available to all parties. The defense team – which was composed by three lawyers – asked the prosecutor's office to access the entire collection, which was later handed to the defense on a hard disk; the material, however, could have been read only through the same analysis software that the police used. The defense applied to the Regional court with two alternative asks: in the lawyer's opinion, the State should have either directly bought a license for the defense, either reimbursed the team for the expense. The court rejected the application, affirming that it was not responsibility of the court to provide the defense team with the appropriate technical tools; the state would have a responsibility to do so only if the inaction would infringe upon the right to a fair trial and the principle of equality of arms, which could be violated if the software was not available on the free market, if the defendant could not afford the cost or if the defense would be faced with disproportionate financial burdens. The Regional Court found that none of the conditions occurred in this case. A readable copy of the full collection was later handed to the defense team. The European Court of Human Rights found no violation of art. 6 of the Convention.

4. *Specialization of Investigative Bodies*

The inhomogeneity among Constitutional and regulatory frameworks is reflected, in the examined countries, also in structural divergences concerning the organization of investigative powers.

These differences, which have a great practical impact, are perhaps the most blatant sign that national legislators have not yet

[12] ECHR, 25 July 2019, Rook v. Germany.

made up their minds on the best way to deal with digital forensics investigations. In this sense, interesting insights emerge from the comparative study: First of all, the coexistence of different approaches is only partially traceable to the traditional distinction between accusatorial and inquisitorial models. When it comes to digital evidence, indeed, how each State decided to address the need to cope with limited human and facility resources seems to be an - at least - equally significant factor.

At the same time, the lack of a comprehensive common approach to this matter does not prevent Member States to share some very relevant policy choices [13]. With regard to investigative powers organization, the most important one seems entrusting the processing of digital evidence to law enforcement bodies with a certain level of specialization. Such a result should not be underestimated, especially in criminal law: Although long invoked, it remains actually mostly hypothetical in many instances which, for example, share with digital forensics a transnational and technical dimension (for instance, financial investigations [14]).

Practical solutions adopted by the examined countries, at least in the antifraud matter, however, rather vary. In Spain, for instance, the law recognizes IT forensics units as a specialized section of the *policía científica* [15]. The same goes for Luxembourg, where the *Service nouvelle technologies* (SNT) is part of the *police judiciaire* according to statutory provisions [16], and in the Netherlands, where a Royal Decree determines the specialists' competence and qualification [17]. In Germany and Italy, on the other side, the

---

[13] Stressing such aspects and the importance of achieving a harmonized approach, *infra*, M. CAIANIELLO, *Conclusive remarks*.

[14] Cf., especially with regard to banking investigations, G. LASAGNI-I. RODOPOULOS, *A Comparative Study on Administrative and Criminal Enforcement of Banking Supervision at National Level*, in S. ALLEGREZZA (ed), *The Enforcement Dimension of the Single Supervisory Mechanism. The Interplay Between European and National Law*, CEDAM, 2020, at § 3.3.

[15] See *supra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 4.

[16] See *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 1.

[17] Besluit of 28 September 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Staatsblad 2018, 340, entered into force on 1 March 2019 (hereinafter "Royal Decree on Investigations in Automated Devices").

existence of law enforcement digital forensics specialists in this matter appears more the result of an internal organization of police bodies [18].

Another significant difference emerges with regard to the involvement of the specialized bodies in the overall investigation. Ensuring a certain separation between law enforcement in charge of the investigation and those entrusted with technical tasks can indeed contribute in reducing the impact of *tunnel vision* phenomena [19]. This appears especially pivotal in the field of digital forensics, where evidence can be so easily tampered with, even unintentionally [20]. A strict distinction in this sense may be however observed only in some countries (Germany, the Netherlands, and, with exceptions, Spain [21]).

4.1. *"Basic" vs "Complex" Digital Forensics Operations*

In the examined countries, the most popular criterion to allocate specialized forces can be identified in the distinction between "basic" and "complex" tasks, although in none of such legal systems the paradigm is clearly defined.

The idea behind this allocation criterion is that the first, and allegedly simpler, phases of digital forensics investigations (mainly, seizure of the device or collection and acquisition of digital data) should be left to "ordinary" law enforcement, while the intervention of specialized bodies should be required exclusively for the most complex operations [22].

---

[18] See *supra*, S. Gless-T. Wahl, *The handling of digital evidence in Germany*, § 3.1, and L. Bartoli-G. Lasagni, *The handling of digital evidence in Italy*, § 3.1.

[19] Highlighting the critical profiles related to the tunnel vision, see C. Meissner-A. Kassin, *Confirmation Biases*, in G.D. Lassiter (ed), *Interrogations, Confessions and Entrapment*, Springer, New York, 2004, p. 197 ff.; K. Findley-M. Scott, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, in *Wisconsin Law Rev.*, 2006, p. 291 ff.; I.E. Dror-D. Charlton-A.E. Péron, *Contextual Information Renders Experts Vulnerable to Making Erroneous Identifications*, in *Forensic Science International*, vol. 156 (2006), i. 1, p. 74-78.

[20] Extensively on the fragility of digital evidence see *supra* R. Brighi-M. Ferrazzano, *Digital Forensics*, cit., § 1.

[21] S. Gless-T. Wahl, *The handling of digital evidence in Germany*, § 3.1; L. Bachmaier, *The handling of digital evidence in Spain*, § 4; for the Netherlands, see Explanatory Memorandum on the Royal Decree on Investigations in Automated Devices, Stb. 2018, 340, p. 35 and Tweede Kamer, 2015-2016, 34372, nr. 3, par. 2.1. under 3.

[22] On the distinction between the two main phases of digital forensics

The decision to apply expert personnel to a case, as well as the very definition of "complexity" in this regard appears, however, a matter of discretion, either in the hands of the prosecutor (Germany), or of the same police (Italy, the Netherlands, and, to a certain extent, Spain) [23]. On one side, such discretion is problematic, as it makes difficult for defendants to successfully claim before the court that their cases were "complex enough" to justify the intervention of specialized teams. From this perspective, therefore, a clarifying effort of national legislators seems urgently required.

On the other side, however, preserving a certain flexibility in the current allocation system seems equally necessary. What emerges from the national reports is indeed that digital forensics investigation is clearly a field in which, perhaps more evidently than any other, resource availability becomes a constituent element for the effectiveness of procedural rights. The issue reveals itself in a preponderant way in this context, because digital forensics specialists, as well as digital forensics laboratories [24], are relatively limited in number. They cannot therefore be reasonably applied to all cases in which that would be required.

It is true that a similar consideration is not exclusive of digital investigations, but could be extended to most scientific evidence. Though in lack of statistical studies on the matter, especially concerning Europe, the impression is however that digital forensics is a type of science which has become much more necessary than other kinds of expertise have. To put it in other words: While DNA or ballistic examinations may be relevant for certain type of cases, digital evidence seems to date an essential element in most administrative or criminal investigation. The need to resort to digital forensics is, therefore, increasingly looking more like the rule, rather than the exception.

Against this background, it seems therefore unrealistic to establish

---

investigations and for a detailed description of each of the latter, cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 5.

[23] See *supra*, S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 3.1; and L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 3.1; for the Netherlands, cf. *supra*, footnote 21. In Spain, the matter is not regulated by the Criminal Procedure Code but, at the same time, internal protocols are rather clear in when and how to involve IT experts. Partially exceptional, against this picture, seems instead Luxembourg, where the *SNT* is reportedly already involved in the execution of seizure orders, cf. *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

[24] For which cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 6.

a rule according to which specialized units shall be involved any time digital investigations are concerned. Such a provision would indeed result in a merely illusory right, available on the book, but *de facto* ineffective in practice.

As it will be further illustrated (§ 4.3), moreover, while regulating a fair and efficient use of specialized forces is imperative, the most vulnerable phases of digital investigations, at least in the defence view, occur in early stages, where IT specialists are usually not yet involved.

4.2. *Training*

A central factor that contributes in both making digital forensics investigation possible and costly (in terms of human resources) is training. Being already analyzed in previous Chapters [25], this issue will be dealt with here only to the extent necessary to point out its impact on the effectiveness of defence rights.

Although widely recognized in principle, the need to properly train law enforcement to make sure agents possess the necessary expertise to handle digital evidence, is subject to quite some divergent implementing approaches in the examined countries.

In Spain, Italy and Germany training programs do exist, but they heavily depend on the discretion of either police academies, universities (master programs), or on the internal guidelines of each law enforcement agency. The efficiency of these solutions appears rather diverging: Completely internal programs might risk being too condescending towards the pupils; on the other side, exclusively university programs require sufficient economic resources to be developed which are not always easy to assemble. Mixed solutions also have to struggle with the need to ensure substantial quality, besides for formal labels.

Regardless some attempts for standardization, moreover, in these countries training programs appear flexible, but also rather scattered and hardly comparable with each other. A different approach is followed in the Netherlands, where training procedures are standardized and established by Ministerial dispositions [26].

---

[25] *Ivi*, § 4, also detailing the possibility to certify such expertise.

[26] Cf. L. Bartoli-G. Lasagni, *The handling of digital evidence in Italy*, § 3.1; for the Netherlands, cf. Regeling van de Minister van Justitie en Veiligheid van 15

Yet another case, conceptually opposed to the previous ones, is that of Luxembourg: There, it is not police that is trained to acquire IT competences, but IT experts are recruited from outside police organizations and then trained in the legal matters to become police officials [27].

Obviously, the mere existence of training programs is not *per se* sufficient to ensure that digital forensics operations will be correctly performed. Especially in the defendant's perspective, what really matters is that the specific agent(s) which carried out the investigation in her case possessed the necessary expertise to do so.

In this regard, becomes therefore pivotal whether defendants can access to the relevant professional qualifications of the involved law enforcement, and whether potential lacunas may be effectively be asserted at trial.

4.3. *Challenging Police Expertise: The Problem of First Responders*

In the examined Member States, the right to access to law enforcement expertise qualification is only rarely recognized (namely, in Spain) [28].

This consideration holds true even though in all legal orders the defendant can usually challenge the admissibility of the evidence produced against her, raising potential critical issues which may include also the investigators' negligence or lack of expertise.

Challenges of this sort are however reportedly not a common practice in any of the examined countries. Several explanations could be suggested in this regard.

A first option could be to conclude that the absence of the right to access to law enforcement qualification, impedes the defendant to collect enough information to successfully raise the issue at trial. The situation seems however alike also where this right to access is actually guaranteed (Spain).

It could thus be argued that defense complaints are limited because police expertise is actually adequate. Empirical research

---

February 2019, kenmerk 2429311, houdende regels betreffende de kwalificaties van opsporingsambtenaren die door de korpschef kunnen worden aangewezen als lid van een technisch team, Staatscourant 2019, 10910.

[27] Cf. K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

[28] Cf. *supra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 4.

should however be carried out in this regard, to understand to which extent this presumed satisfactory level of expertise could be considered a direct consequence of the transparency approach adopted in the Spanish legal system. In other words: To confirm this hypothesis it should be highlighted whether a similar level of trust could be found also in countries where police is not bound to provide proof of its technical expertise.

A further potential explanation may also be raised. A generalized reluctance of defense lawyers to directly challenge the "personal" qualification of law enforcement could be also an effect of the lack of adequate training of lawyers and judges themselves in this matter. Properly trained lawyers could be more prone to denounce potential violations in the handling of digital evidence. Properly trained judges, on the other side, could be more likely to sustain such issues, as they would better understand the relevance of the underneath reasoning [29].

In the equation, anyway, there is a last, crucial factor to be taken into account.

As anticipated (§ 4.1), specifically trained law enforcement agents are usually applied only to the "complex" steps of digital investigations – mainly the analysis of the collected data – or, at most, to cases that since the beginning appear rather delicate. This is not, however, the phase of digital investigations in which police inexperience could display its most irreparable consequences.

In all kind of investigations (not just those involving digital evidence), information gathering, at the "crime scene" and in its proximity, is actually the context where investigators are more likely to commit mistakes that could impair the whole following procedure [30].

---

[29] With regard to lawyers, a role in this sense could also be played by the the so-called *local legal culture*, that is when a counsellor tends to consider imperative to preserve good relationships with local institutional actors (such as police), even when that reduces her client in a *transient and socially remote character who is unlikely toinfluence prevailing outlooks.* For an overview of the detrimental consequences of this approach, cf., for instance, C. WALKER-K. STARMER, *Miscarriages of Justice. A Review of Justice in Error*, Blackstone Press Limited, 2nd ed., 1999, p. 9 ff; G. DI FEDERICO-M. SAPIGNOLI, *I diritti della difesa nel processo penale e la riforma della giustizia. Le esperienze di 1.265 avvocati penalisti*, CEDAM, 2014.

[30] Cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics,* cit., § 1 ff.; M. DANIELE, *Prova scientifica e regole di esclusione*, in G. CANZIO-L. LUPARIA (eds), *Prova scientifica e processo penale*, CEDAM, Padova, 2017, 490.

In digital forensics investigation, this phase is generally handled by "ordinary" law enforcement, and not by specialized units. Against this background, the bottom question at stake should be rephrased in whether any guarantee has been established to ensure to the defendant, that *such* agents possess the skills to adequately perform these very first, and essential operations.

It has been previously argued, indeed, how Phase 1 of digital forensics investigation requires a certain awareness and experience to be correctly performed [31]. None of the examined Member States, however, offers a clear legal framework (when not any regulation at all) in this regard [32]. Actually, besides for a few general recommendations that also agents acting as First Responders should possess basic IT knowledge [33], no guarantee is reportedly offered to the defendant that this will occur in her specific case.

Thus, the adoption of standardized and mandatory basic training programs emerges as an absolutely crucial and urgent necessity, to confer effectiveness to both defence rights and best practices. To this end, a possible solution could pass through the official adoption of the ENFSI First Responders guidelines [34] for the training of "ordinary" law enforcement.

5. *Digital Forensics Consultants*

Compared to the specialization of investigative bodies, regulations concerning private digital forensics consultants appear more uniform in the examined Member States.

Been listed in a specific public registry is generally mandatory for consultants in Spain and Italy (although only in the first case this is subject to specific quality checks to ensure candidates possess the specific expertise required [35]). In Germany and Luxembourg, on the

---

[31] Cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 5 ff.

[32] Perhaps with the exception of Luxembourg, where, as illustrated, law enforcement digital experts are reportedly systematically involved in the investigations since the search and seizure, cf. *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

[33] As recommended, for instance, in Italy, cf. L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 3.1.

[34] On which see *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 3.1; although Luxembourg is not a member, cf. K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

[35] Cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 4.

other hand, the law does not impose a certification. Registries of (sometimes privately certified) experts are nonetheless in place, from where courts or prosecutors may appoint a consultant [36].

In this context, therefore – perhaps with the exception of Italy [37] – information about the expertise of the appointed consultant is overall rather accessible to the defendant, who may raise related complaints at trial.

It is however not just institutional actors that may outsource part of their activity to private parties: Digital forensics consultants can indeed by appointed also by the accused, during the investigation, or at trial.

As will be further illustrated (§ 6.2), this right is recognized, in different forms, in all the examined countries.

Regardless of this theoretical recognition, though, most national reports highlight how the concrete chances for the defendant to exercise it are heavily dependent on the availability of adequate economic resources [38].

The issue is obviously not limited to digital investigation, as it can potentially extend to all situations in which a technical expertise is required. However, the impact of limited resources potentially bears a heavier burden in this field, compared to other scientific sectors: As anticipated, the pervasiveness of digital technology in our society is indeed such, to make digital investigations relevant in almost every investigation.

Also in the perspective of the defence, therefore, this change of paradigm, still rather underestimated at the normative level, needs to be urgently taken into account, not to make the exercise of defense rights purely illusory.

6. *Defence Rights*

Despite the implementation in all Member States of the Budapest Convention, in none of the examined countries, a comprehensive set of defence rights may be observed, that has been established precisely for

---

[36] Cf. *supra*, S. Gless-T. Wahl, *The handling of digital evidence in Germany*, § 3.1; K. Ligeti-G. Robinson, *The handling of digital evidence in Spain*, § 2.

[37] Cf. *supra,* L. Bartoli-G. Lasagni, *The handling of digital evidence in Italy*, § 3.2; R. Brighi-M. Ferrazzano, *Digital Forensics*, cit., § 4.

[38] *Supra*, S. Gless-T. Wahl, *The handling of digital evidence in Germany*, § 2; L. Bachmaier Winter, *The handling of digital evidence in Spain*, § 5.1.

digital investigations. A partially different perspective may be found only in Germany, where a specific fundamental right has been recognized by the Constitutional Court, to protect the individual privacy in its virtual dimension [39].

Such lack of a comprehensive approach among Member States, moreover, is far from representing a homogenous approach.

At a closer look, it may be observed that a few tailored provisions actually exist in most of the examined legal systems, though rarely concerning the same procedural profile. In other words, as it will be briefly illustrated below, while some States intervened only to "update" information and access rights (§ 6.1), other States chose to amend only the right to be heard (§ 6.2), and others, finally, did not make any formal amendment at all. The picture is then even more scattered when it comes to available remedies against procedural breaches occurred in digital forensics investigations (§ 6.3).

6.1. *Right to Information and Access to File*

In most of the examined Member States (Germany, Italy, Luxembourg, and Spain) the right to information and to access to file concerning digital forensics investigations are recognized through an extensive application of the provisions originally established for "analogue" investigative acts.

Although rather neutral in principle, this approach can generate several inequalities in its implementation, mainly due to the difficulties in framing new investigative tools in a legal framework clearly tailored on a physical dimension. A clear example in this sense comes from Germany, where the uncertain allocation of digital investigations between *open* or *covert* investigative measures can result in an uneven recognition of procedural safeguards, and of information rights, which is strongly criticized by legal scholars [40].

Against this general background, a distinctive arrangement can be found in the Netherlands, where digital searches are officially attached with specific information obligations.

In particular, if data is recorded or made inaccessible as a result of

---

[39] See *supra*, S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 1.3.

[40] For which different sets of procedural rules apply, see S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, §§ 2.2-2.3.

a search, the "persons concerned" shall be notified in writing, as soon as possible, of the latter, and of the nature of the data recorded or made inaccessible. Such a notice may be postponed if the interest of the investigation so requires [41].

6.2. *Right to be Heard*

Contrary to the case previously examined, inhomogeneity among regulations on the right to be heard tends to follow the traditional distinction between accusatorial and inquisitorial systems.

In this regard, it can first be observed how in countries with more accentuated accusatorial features, like Italy and (at least in this regard) Spain, the defendant has the right to appoint a (digital forensics) consultant to challenge the prosecutorial or court expert witness. On the other side, traditionally inquisitorial system like Germany, only allow the defendant to request the court to appoint an expert witness [42]. In Luxembourg, however, the defendant is entitled to appoint her own consultant to attend the operations of the investigating judge's consultant, as long as this is not reckoned to delay the work of the latter [43].

Secondly, and perhaps more relevantly for the present study, it could be noted that (more) accusatorial models appear to have implemented (Spain), or to be trying to implement (Italy [44]), some "enhanced" form of participation for the defendant also in the very first phases of digital forensics investigations.

Especially interesting, in this regard, is the Spanish regulation, according to which the cloning of digital data shall be performed not only at the presence of the defendant, but also of a third, neutral

---

[41] Section 125m ff, Dutch Criminal procedure code, according to which "persons concerned" may be defined as: a. the suspect; b. the person responsible for the data; c. the person entitled to use a place where a search has been conducted.

[42] Cf. *supra*, S. Gless-T. Wahl, *The handling of digital evidence in Germany*, § 3.3.

[43] *Supra*, K. Ligeti-G. Robinson, *The handling of digital evidence in Luxembourg*, § 2.

[44] Although still far from established, in Italy some case is slowly starting to emerge, in which the acquisition of digital data or the decision on how to search such data (*e.g.* keywords) is performed in compliance with the accusatory principle, even in the pre-trial investigation phase, either in the forms of *accertamenti tecnici irripetibili* or of *incidente probatorio*, see *supra*, L. Bartoli-G. Lasagni, *The handling of digital evidence in Italy*, § 2 and § 3.2.1.

party, entrusted to guarantee the correctness of the operations carried out by the investigators (*Letrado de la Administracíon de Justicia*) [45].

Such "enhanced" mechanisms are, on the other side, tendentially lacking in inquisitorial systems.

Partially eccentric to this otherwise clearcutting separation is however, again, the case of Luxembourg. Even in the absence of legislative provisions, in fact, a participated procedure has been reportedly developed in the domestic case-law.

According to this jurisprudence, all parties (defendant and her counsellor, police and investigating judge) are to agree in advance and in writing about the procedure to be followed for the acquisition of digital data (where to keep the digital devices, which security measures to apply, who is to be present during the actual search of the devices, the procedure to exclude and destroy the irrelevant material...) [46].

In principle, this procedure could represent a rather good model for all the examined Member States, also where some provisions to allow a greater level of participation to the defendant have already been introduced. In light of the considerations illustrated above, however, it is worth mentioning that even in Luxembourg, the implementation of this method on a systematic basis raises several sustainability concerns, in terms of employed facilities and personnel [47].

6.3. *Remedies*

In none of the examined countries, specific remedies have been established in case of breach of technical standards or of procedural rules relating to digital forensics investigations. Ordinary remedies thus apply also in this regard, which are implemented in rather diverging ways by Member States.

A first option, shared by most legal systems, is that of providing

---

[45] Article 569 LECRIM, cf. *supra*, L. BACHMAIER, *The handling of digital evidence in Spain*, § 5.1, highlighting how according to the case-law, for cloning this safeguard is not required, as hash function is deemed sufficient to guarantee the correctness of the operations.

[46] *Chambre du conseil*, Cour d'appel, 11 November 2014, no 824/11, cf. *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 1, p. 18.

[47] Cf. *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 1, p. 18.

for exclusionary rules when evidence is collected in violation of criminal procedure provisions [48]. Often, though, the capacity of such mechanisms to offer an effective remedy is watered-down by an excessive degree of discretion by the proceeding authority, or by a limited scope of application of the norm.

In Luxembourg, for instance, exclusionary rules for violations of domestic statutory law, as well of Article 6 ECHR, may be invoked in the pre-trial phase. However, no specific standard is provided for in the legislation to clearly define where such sanction shall apply. The decision, therefore, entirely relies on a case-by-case assessment of the pre-trial chamber [49].

Even more evident the Dutch case. Where a violation occurs during the pre-trial investigation that cannot be repaired at a later stage, excluding the evidence obtained is only one of the potential options applicable by the courts, and by far the least used. Instead, breaches of defence rights are more commonly addressed by reducing the final sentence "correspondently" to the degree of the occurred violation [50]. This solution seems however quite unsatisfactory, especially when compliance with fundamental rights is at stake.

Against this background, peculiar is the approach adopted in Spain, where not only exclusionary rules are applicable to all evidence obtained in violation of fundamental rights, regardless of the moment in which the violation occurred, but also the criminal liability of public officials could be invoked. This last option may concern, among others, the case in which public officials do not comply with the procedural safeguards established by the law, for instance during searches [51].

A second approach that finds application is some of the examined Member Stats is to grant the defendant the right to judicial review, immediately after the completion of the investigative measure. Also in this case, however, critical features have been reported, which risk to severely undermine the effectiveness of such remedies when digital investigations are at stake.

---

[48] For general systemic considerations on the matter and literature references, see *infra*, M. CAIANIELLO, *Concluding remarks*.

[49] See *supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 3.

[50] Cf. Section 359a, Dutch Criminal procedure code.

[51] See *supra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 5.4.

Relevant, in this sense, is the case of Germany, where this right is provided for by statutory law only against *covert* investigative measures. When digital forensics operations fall under the label of *open* investigative measures, the possibility to trigger a judicial review relies entirely on conditions established by the case-law. It moreover varies depending on who is the authority who ordered the measure, and is subject to the demonstration of a legitimate interest by the defendant [52].

Also significant in this regard is the case of Italy, where, for instance, the possibility to trigger a judicial review just after the completion of a (digital) search bears relevant limitations in its scope. Procedural violations are indeed not considered relevant if the search has brought to the seizure of the *corpus delicti*. The right to an (immediate) judicial review, moreover, does not apply at all where the search (and therefore the interference in the privacy of the person) has been carried out, but no seizure has been ordered [53].

Finally, a third option, often added to the previous ones, is that of ordering the destruction *without delay* of the data which has been illegally collected. This remedy seems in principle conveniently tailored for digital forensics investigations, as it can apply (*e.g.*, in Germany [54]) not only in case of direct violations of procedural rights, but also when data has been collected in violation of privacy rights (*i.e.* where the data are irrelevant to the proceedings) [55].

Considering too risky to employ such a "drastic" measure before the conclusion of the proceeding, however, many legal systems opted for a compromise, ruling for the conservation of a backup copy of the complete data until the decision becomes final [56]. Although reasonable

---

[52] See *supra,* S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, §§ 2.2-2.3.

[53] Cf. *supra* L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 4.3.

[54] Cf. *supra*, S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 5.1.1 referring to Federal Constitutional Court (BVerfG), Decision of 12 October 2011 - 2 BvR 236/08, in *Neue Juristische Wochenschrift (NJW)* 2012, 833, 838 (mn. 220) (Ger.).

[55] Cf. *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit. § 7, highlighting that, anyway, this measure «has nothing different from the excerpt of wiretapping, or release from the seizure of any kind of finding (a car, a flat...)».

[56] *E.g. supra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 3; L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, § 3.5, *sub* e), p 15; the same for Italy in case of interception of communications (Article 269 c.p.p.).

in the perspective of the investigators, this solution, supporting a rather high degree of tolerance towards afterthoughts on the investigative side, sensibly reduces the effectiveness of this remedy for the defendant.

7. *Third-Party Rights*

Especially if compared to the position of the accused, third parties with a "legitimate interest" in the performance of digital forensics investigations, enjoy a fairly uniform status in the examined countries.

Despite the absence of a harmonized definition of such "legitimate interest", most Member States indeed recognize these subjects the right to complain against (digital) searches and to ask for the restitution of the seized data or device. An exception in this sense emerges in the Netherlands, where third parties cannot activate this remedy; however, if the targeted data are not originating from the accused or not addressed to the latter, their recording requires a previous judicial authorization [57].

In most cases, moreover, third parties are equated to the position of the defendant with regard to certain specific powers.

In Luxembourg, for instance, third party rights extend also to the possibility of requesting the investigating judge to appoint an expert consultant [58]. In Spain, on the other side, also third parties can press charges against public officials that infringed their rights, carrying out the investigative measures in violation of procedural rights (see above, § 6.3). Again in Spain, but also in Germany and Italy, third parties with a legitimate interest are recognized the right to information and the right to be heard in terms equal to those of the accused.

Lastly, in Luxembourg, third parties have an impact also in determining the range of potential operations carried out by law enforcement in the first steps of digital investigations. Where the targeted data are stored on a server along with data of other persons not involved in the investigation, police is indeed prevented from seizing the device. In light of the proportionality principle, law

[57] Cf. Section 125la, Dutch Criminal procedure code.

[58] See *supra*, K. Ligeti-G. Robinson, *The handling of digital evidence in Luxembourg*, § 3.

enforcement should rather make a copy of the data, leaving the device in its original location [59].

8. *Admissibility at trial*

All systems consistently stress one point: digital evidence ought to be reliable and, to ensure its authenticity, all systems have accepted to trade-off proportionality at least to some degree. However, this attention seems to fade when it comes to admissibility at trial. None of the concerned legal systems have specific rules on the admissibility of digital evidence, nor they show a particular connection with the reliability of the item.

On this subject, these European legal systems seem to widely differ from the U.S. way of dealing with authenticity and admissibility. The U.S. Federal Rules of Evidence state that the proponent of a piece of evidence «must produce evidence sufficient to support a finding that the item is what the proponent claims it is» [60]. This requirement has been historically satisfied with a precise paper trail on every item, detailing its collection, transfer, analysis, custody. The same documentation requirement has been applied to digitally stored information: it can be presented as evidence, but it should come with a so called "chain of custody" to vouch for its authenticity. Technical standards and documentation duties are in close connection with the possibility to use the material at trial; there are other ways to authenticate it, but a complete chain of custody is still the best assurance: if the history of the material is not clear, the proposed evidence could be discarded as unreliable.

European legal systems have undoubtedly inherited the emphasis on the reliability of digital evidence, also thanks to the baseline that the Budapest convention has established since 2001, but have not provided for the same solutions. Few of the involved countries have technical standards in place; only Spain has a complete set of guidelines that should be consistently applied by police. Moreover, there are no exclusionary rules: the unreliable evidence can be admitted and used at trial; it is incumbent upon the interested party to discredit the piece of evidence, not upon the proponent to show that it is in fact

[59] *Ivi*, § 1.
[60] U.S. Federal Rules of Evidence, n. 901.

reliable. Accordingly, the judge will have to evaluate the evidence and rule on its trustworthiness.

Similar settings, therefore, should push even harder on a sound chain of custody. Challenging the item is only possible if all operations are either repeatable – which can prove difficult, or even impossible – either reported down to the last detail. However, this has not been the case so far. The only legal system that has strict reporting obligations in place is Spain: UNE guidelines contain an obligation to record every operation, either digitally either through a paper-based document management system. The Dutch legal system has a similar obligation in place, but only for covert investigation techniques such as online searches. The documentation requirements for "ordinary" searches and seizures are not that severe, although they are the main entry for digital evidence at trial.

The Italian and the Luxembourgish systems have a traditional French-style duty to draft up a written report for almost every police operation. However, the law does not demand for particular details when a mass-storage device is involved: a satisfying report, for instance, could just contain the mention of a mass-storage device being seized. In both countries, however, police forces are working on stronger reporting obligations. It may appear as a paradox: the subject proposing stricter standards is the one that could lose more from a narrower margin of appreciation; showing a clear record, though, can boost the credibility of the evidence and spare time in litigation. On the one hand, it helps holding the practitioners accountable and works in favor of the defense; on the other hand, it can make the investigator's case stronger.

The Italian *Guardia di Finanza*'s guidelines requires that the agents draft up the legally required report and an additional document called "chain of custody", that should contain a list of seized files – identified by hash value – and record every operation performed on the data set as well as every transfer. The practice clearly mirrors the U.S. practice, but it is worth pointing out that the document is not mandated by law; its absence – or the lack of full traceability of operation – cannot be used to argue for the exclusion of the item. In Luxembourg, the police are working on a "follow-up informatic", a practice intended to keep track of the evidence management and its storage location.

Turning to administrative proceedings, none of the analyzed systems contemplate specific admissibility criteria.

9. *Production of digital evidence in different proceedings*

The flow of evidence can proceed in two directions: form administrative to criminal; criminal to criminal [61].

Each of these situations poses a different threat that all legal systems have faced. During administrative proceedings, data that would be privileged have to be disclosed; the target of the investigation does not necessarily enjoy a full set of rights as she would under a criminal proceeding. Therefore, the course of information can be stopped, at least in some cases, or subjected to conditions. In Luxembourg, what has been gathered during an administrative proceeding can be admitted at a criminal trial as long as it has been collected in a loyal manner and it is debated adversarially. In Italy, evidence gathered during an administrative proceeding is admissible at a criminal trial as a document; however, if the administrative authority recognizes the elements of a crime, it shall proceed according to the rules of the code of criminal procedure. The German legal system provides for another type of limit: evidence collected in tax proceedings cannot be used in a criminal trial if it was produced under the obligation to disclose fiscal information; this shield can be pierced if there is a compelling public interest in bringing criminal charges.

The "criminal-to-criminal" scenario offers a different kind of risks. For instance, the mechanism could be used to circumvent the need for judicial authorization or to restrict the possibility to challenge the material. Every legal system has come up with different limits, that strictly depend on the requirements to resort to the measures in the first place. Thus, in Spain, the evidentiary results of a mass-storage device search and seizure can migrate to a different criminal proceeding only upon authorization of the investigating judge, that can be issued at the request of the public prosecutor and if all the legal prerequisite are met. The Italian legal system, as mentioned above [62], does not have the same authorization system in place; however, it poses terms and conditions to the production of evidence in other criminal trials. Evidence can freely

[61] Administrative to administrative will be overlooked at this time; normally, in all countries, the administration can issue production orders that would compel other branches of the administration to forward all relevant documents in their possession. The variety of imaginable scenarios and the structural differences between countries are too wide to be fully detailed here.

[62] See § 1.

circulate if they were assumed during the trial or during a special evidentiary hearing, where both parties can debate in front of a judge; or if it is impossible to fruitfully re-assume the evidence. Oral evidence can only be used at another trial if the defendant's lawyer had a chance to cross-examine the witness in the original proceeding. In Germany, the courts and the prosecutors can share information they deem necessary to pursue criminal or regulatory infractions. If data is gathered through a measure that can be authorized only for a certain set of crimes (i.e.: covert measures), then it can only be used with the consent of the defendant, or if the proceeding would have justified the adoption of such a measure anyway; searches and seizures, however, are not among these tool.