Conclusive remarks. Antifraud investigations and respect for fundamental rights faced with the challenge of e-evidence and digital devices.

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

Alberto Camon

THE PROJECT DEVICES AND DIGITAL EVIDENCE IN EUROPE

We all know how digital technology has irreversibly changed our daily lives: we normally interact with IT-tools to achieve private goals but also to manage our relations with public and private institutions, such as banks or governmental agencies. The COVID-19 pandemic further accelerated the rush to digital-only services, for in-person interaction suddenly became dangerous. E-commerce, online assistance, digitalized payment methods, e-Government went from being an option to being necessary for businesses to run, and for individuals to stay safe [1]. The World Health organization itself recommended to use as little cash as possible, in order to prevent the spread of the virus [2]: a traditional and somewhat controversial claim of the anti-money laundering experts was accepted overnight as a precautionary measure. At the same time, all administrations were forced to boost their online services, as more and more people and companies were filing for state programs; what required an in-person meeting had to be rapidly rearranged to happen remotely [3].

This comprehensive, massive shift towards digital models has been generating a useful side product: data, that has become a valuable resource in itself.

Even the fight against fraud has been reorganized around IT-tools and digital information: every step of the anti-fraud cycle – prevention,

---

[1] For some data, see L. Alderman, *Our Cash-Free Future Is Getting Closer*, in *nytimes.com*, 6 July 2020.

[2] B. Gardner, *Dirty banknotes may be spreading the coronavirus, WHO suggests*, in *telegraph.co.uk*, 2 March 2020.

[3] On the topic, see *COVID-19: How eGovernment and Trust Services can help citizens and businesses*, in *ec.europa.eu*, 24 March 2020. According to the official website, more than a quarter of the active electronic IDs in Italy (SPID) were issued in the first semester of 2020: see *avanzamentodigitale.italia.it*.

detection, investigation and prosecution, recovery – is either powered by informatic portals, or heavily relies on digital material.

Fraud prevention is almost entirely managed through data collection and analysis, which allow to identify patterns and create risk profiles; the system can figure out indicators for fraud, that can trigger early warnings. This technique helps mapping the territory and rationalizing resources: it permits to identify the most risk-prone areas and deploy resources accordingly. The audit and control effort can therefore be better focused, and its results maximized. That is why, in its 2019 antifraud strategy, the European Commission stressed the point even further: its «Objective n. 1» is to build its data-analysis capacity even further [4]. The member states are also drafting their own anti-fraud strategies and developing similar mechanisms [5]: Italy, for instance, has implemented the National Anti-fraud Database (D.N.A.), a tool that can quickly merge information and create a risk score for individuals and companies [6]. The planning of routine controls is then drafted also according to the red flags that the system raised.

The following step of the cycle – detection – is also based on a data-sharing platform, the Irregularity Management System (IMS). It collects data on signaled anomalies, suspect activities and established wrongdoings, helping the dialogue between OLAF and member states [7].

In the first two stages, data are used to build a compass for the law

---

[4] In particular, the European Commission underlined the need for «a more comprehensive central analytical capability so that it can scan data on fraud patterns, fraudsters' profiles and vulnerabilities in EU internal control systems»: *Commission Anti-Fraud Strategy: enhanced action to protect the EU budget*, COM(2019) 196 final, 29 April 2019, in *ec.europa.eu*, p. 9. The point is further detailed in an accompanying document: *Commission Staff Working Document – Fraud Risk Assessment*, SWD(2019) 171 final, 29 April 2019, in *ec.europa.eu.*

For an overview, see also: C.A. MAKRI-O. MARIN, *The Commission's New Anti-Fraud Strategy – Enhanced Action to Protect the EU Budget*, in *Eucrim*, 2019, p. 218 ss.

[5] See OLAF, *Practical steps towards the drafting a National Anti-Fraud Strategy*, 7 December 2015, in *ec.europa.eu*, which also mentions data and IT-tool as instrumental to the fight against fraud.

For the Italian approach, see COLAF, *Relazione annuale 2018*, in *politicheeuropee.gov.it*.

[6] For more on the software, see *Database Nazionale Antifrode*, 2016, in *politicheeuropee.gov.it*; or, in English: *Guidelines on a National Anti-fraud Strategy*, 13 December 2016, in *ec.europa.eu*, p. 41.

[7] On the tool, see the *Handbook on "reporting irregularities in shared*

enforcement agencies: information helps them moving forward in a reasoned direction, shaping policies and organizational plans. When it comes to the last two phases of the cycle – investigation and prosecution, recovery of the sum – data are still crucial, but they help in a different way. They are not used to support planning or policy shaping, they are instrumental in proving or disproving a case, or to locate capitals. In the first half of the cycle, they are used to predict the future and adequately prepare for it; in the latter half, they help reconstructing the past, unveiling illicit activities and making things right.

Along with the advantages we just summarized, every use of data within the cycle raises a specific set of issues, and DEVICES [8], the European project whose results are published in this book, aimed at facing one of the many challenges in the evidentiary use of digital material, especially in criminal and administrative antifraud proceedings.

The current regulatory setting – both national and international – has been acknowledged as largely unsatisfactory, as it does not provide for specific answers to the peculiar problems that digital evidence entails. Data can be created in Germany, transit through an American server to finally be stored in Ireland, while the person that triggers the entire process has not even left her couch; for this reason, the need for the swift exchange of electronic information has been growing, together with the power of private corporations that manage data. The legislatures are slowly reacting and, as a result, digital evidence has become a genuine "hot topic": every international organization is coming up with proposals, templates, regulations to expedite the mutual legal assistance on the subject. The European Union is working on private-public cooperation, that could advance through the proposal about European production and preservation orders [9]; the UN is establishing a dedicated section on the SHERLOC

---

management", 2017, in *politicheeuropee.gov.it*; *User Manual 2: IMS-users and their role*, 24 October 2018, in *politicheeuropee.gov.it*.

For the Italian policies on fraud signaling, see *Linee guida sulle modalità di comunicazione alla Commissione europea delle Irregolarità e Frodi a danno del bilancio europeo*, 2019, in *politicheeuropee.gov.it*.

[8] Its full title is «Digital forensic EVIdence: towards Common European Standards in antifraud administrative and criminal investigations» and it is funded by the European Union's HERCULE III Programme 2018 – Legal Training and Studies. For more information, see: *site.unibo.it/devices/en*.

[9] Proposal for a Regulation of the European Parliament and of the Council on the European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108 (COD), in *eur-lex.europa.eu.*

portal, with public resources on digital evidence coming from a variety of countries [10]; the Council of Europe is drafting a second protocol to the Budapest convention on enhanced international cooperation and access to evidence in the cloud [11], that would add to the third part of the Convention (artt. 23-35), which is already dealing with international cooperation and is currently in force.

None of these valuable projects, however, seem to have touched upon a key problem: the quality of what is to be exchanged. None of the proposals, to this date, contain a single provision on how to reliably collect, analyze and present the material. This approach is of course not a sign of indifference; nonetheless, it may be a symptom of a common misconception that holds all data as equally reliable, for they cannot lie. Forensic science in general and computer technology in particular are often presumed as being absolutely trustworthy [12]: they appear to offer little or no possibility for tampering, or for human interaction altogether; devices do not get confused, do not misremember or misinterpret. The collective opinion would say: the machine can only offer an objective representation of the truth, for «there is no such thing as a mechanical lie» [13].

This issue is just one of a thousand problems and paradoxes that we can find while studying digital evidence: on the one side, data are very easy to transfer, and this creates a very strong need for a uniform legal regulation; on the other side, the international layer provides for some principles, but not for specific provisions.

On the one side, crossing borders is very easy in a digital investigation, which should require a constant resort to mutual legal assistance mechanisms. On the other side, these procedures are

---

[10] For more information, visit *sherlock.undoc.org*.

[11] On the subject, see: CYBERCRIME CONVENTION COMMITTEE, *Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime. State of play*, 23 June 2019. See also: CYBERCRIME CONVENTION COMMITTEE, *Provisional draft text of provisions: Language of requests, Emergency MLA, Video conferencing*, 29 November 2018.

[12] The phenomenon has been promoted by popular culture, with tv series that show unbeatable forensic scientists cracking every case thanks to their undeceivable, technical insight: on the subject see J.M. CHIN-L. WORKEVYCH, *The CSI Effect*, in M. DUBBER (ed.), *Oxford Handbooks Online*, New York, Oxford University Press, 2016. It is worth noticing that the popular TV show has also had an IT-themed spin-off: *CSI: Cyber*, with computer analysts represented as infallible heroes tracking down criminals thanks to the absolute reliability of their information.

[13] F. CORDERO, *Procedura penale*, IX ed., Giuffrè, Milano, 2012, p. 581.

cumbersome, slow, disproportionate and the law enforcement agencies have developed strategies to set them aside. The most frequent is probably the direct contact with foreign service providers, that are asked or ordered to produce the information at their disposal: in this way, the main legal resort is effectively circumvented [14].

On the one side, the right to a fair trial requires that the prosecution authorities disclose to the defence all material evidence in their possession. On the other side, the technology allows for the collection and the potential presentation to court of a staggering amount of data. A famous U.S.-case [15] involved 200 terabytes of electronically stored information (one terabyte is generally estimated to contain 75 million pages of Word documents), seized from 600 computers. Implementing countermeasures is not easy [16], but it is clear that the discovery, without counterweights, ceases to be a guarantee for the defendant and devolves in a trap: the defense would be submerged by such a dump of information.

On the one hand, the digital investigation should be conducted by experts; on the other, the situation is often dire and the urgency makes it impossible to wait for an expert.

DEVICES has touched upon some of these paradoxes, but – as mentioned – the project delved in one in particular: on the one side, the use of technological tools projects an aura of reliability; on the other side, electronic material is not always reliable [17]; it is

---

[14] On this issue, 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 Direito Processual Pen.*, vol. 5 (2019), p. 1277 ff.; P. de Hert-C. Pralar-J. Thumfart, *Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to Microsoft Ireland*, in *New Journ. Eur. Crim. Law*, 9 (2018), p. 326 ff.

[15] United States v. Shafer, 2011 WL 977891, N.D. Tex. Mar. 21, 2011.

[16] Is it necessary to make the relevant material searchable? Or at least to class it? Or at least to provide an index? Changing the file format to make it searchable, however, can alter or erase the metadata such as time and location stamps, and modification logs that could be very important. One could think that the prosecutor should disclose two versions of the collected data: the original, with metadata, and the searchable form. But who should pay for the service? For these and other problems, see the brilliant essay by J.I. Turner, *Managing digital discovery in criminal cases*, *Journ. Crim. Law & Criminology*, 109 (2019), p. 237 ff.

[17] Among others, E. Van Buskirk-V.T. Liu, *Digital Evidence: Challenging the Presumption of Reliability*, in *Journ. of Digital Forensic Practice*, 2006, p. 19 f.; E. Casey, *Error, Uncertainty, and Loss in Digital Evidence*, in *Int. Journ. of Digital Evidence*, 1 (2002), § 1 ff.

extremely fragile and it is easy to manipulate [18], since there's a «myriad of possibilities contributing to an undetected error in computer-derived evidence» [19]: programming defects, missing updates, informatic attacks, bad maintenance or use conditions, improper handling or examination... [20].

Against this background, DEVICES aimed to gain a better understanding of the present epistemological framework on digital investigations. The research project has been analyzing the status quo, acknowledging its strengths and identifying the weaknesses, in order to articulate a proposal for a common path forward.

We adopted both a comparative and an interdisciplinary approach, and these methodological choices were, at least to some degree, mandated by the nature of the subject: states must trust one another, which may come easier with a deepened knowledge of national procedures and practices. However, legal solutions must be tested and evaluated also on a technological level: a trained, specialized eye can provide some insight on how digital investigations should be regulated and performed, in order to guarantee the integrity of the material and the reliability of the outcomes.

Therefore, one essay will be entirely devoted to the analysis of the currently available standards, from a digital forensic perspective [21]. It will specify the technical requirements for every stage of the digital investigation: collection of data, analysis, interpretation and presentation of the results. This part of the work is particularly

---

[18] ENISA (European Union Agency for Network and Information Security), *Digital forensics Handbook. Document for teachers*, 2013, p. 3 f., available at *enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook*; ISO/IEC 27037:2012, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, § 5.4.1; N. JONES-E. GEORGE-F. INSA MÉRIDA-U. RASMUSSEN-V VÖLZOW, *Electronic evidence guide* (published in 2013 under the *CyberCrime@IPA* joint project of the Council of Europe and the European Union on cooperation against cybercrime in South-eastern Europe and available at *rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4*), p. 12, 66 ff., 137.

[19] E. E. KENNEALLY, *Gatekeeping Out of The Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence*, in *Virginia Journ. Law & Technology*, 13 (2001), available at: *ssrn.com/abstract=2145644*, § 41.

[20] E. CASEY, *Digital Evidence and Computer Crime*, 3rd ed., Academic Press, Waltham, p. 7 ff.; S. SIGNORATO, *Le indagini digitali*, Giappichelli, Torino, 2018, p. 100 f.

[21] R. BRIGHI-M. FERRAZZANO, *Digital forensics: best practices and perspectives*, *infra*.

useful for who is normally studying statutes and jurisprudence: it can serve as a guide to compare the legal regulation of individual stages, and it suggests workable solutions.

Turning to the legal side of the project, we selected five countries – Germany, Italy, Luxemburg, Spain and the Netherlands – and asked national experts to provide a critical assessment of the current legal landscape from an internal point of view. The study on the Netherlands has remained at a preliminary stage and therefore it is not a part of this publication. However, the interesting results of the work have been taken into account by the digital forensics report, the comparative report and the conclusions.

The first step of the analysis has been dealing with the fundamental rights at stake: which are the most concerned, from where are they derived, how can they be legitimately limited and to what extent. Each of the countries we considered had to reflect on how to update their bill of rights to protect citizens from new forms of state interference, and the first, homogeneous result is quite striking: the most rooted constitutional categories such as the *habeas corpus*, the inviolability of the domicile and freedom and secrecy of communications may prove quite ineffective to properly limit novel entrenchments. The digital age has made unprecedented opportunities available for state surveillance, and the infringement on fundamental rights does not necessarily involve a patrol of agents breaking through the door of the suspect's home. These scenarios have sometimes been handled through innovative interpretations of the constitutional text [22], sometimes relying on international sources such as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

Whatever the technique, all states agree that the right to privacy is affected the most, and that it can justifiably be limited only if the action is proportionate. This frame has been able to stimulate reflection and produce a somewhat careful regulation for covert investigative measures, that are undoubtedly the most intrusive and dangerous. The largest part of the digital material used in criminal and administrative proceedings, though, is collected by means of open measures such as searches and seizures, which have not changed much since their inception.

[22] Famously, the Federal Constitutional Court of Germany chiseled the notion of privacy out of the general concept of human dignity: for more details on the subject see S. Gless-T. Wahl, *The handling of digital evidence in Germany, infra*.

According to a recent survey conducted by the Cybercrime Program Office of the Council of Europe (C-PROC), 82 countries in the world have issued specific regulations of the procedural powers that are necessary to preserve and gather digitally stored evidence, whereas «many states still rely on general procedural law provisions (for search, seizure and so on) to investigate cybercrime and secure electronic evidence» [23]. From a formal point of view, all the nations that DEVICES considered have an unambiguous legal base for the collection of stored data, and they have been counted among the countries that already provided for dedicated procedural powers [24]. Looking at the content of the legal base, however, it is easy to realize how four out of five countries [25] have just extended the traditional regulation of searches and seizures to data and networks, without adapting it to a peculiar object such as digital information. The call for a «new criminal procedure» with regard to digital evidence [26] has remained unheard: at least in this specific domain, the old regulations still discipline a new reality.

As a result, these measures have become more threatening than ever. A good example can be found in a recent decision of the European Court of Human Rights: in a criminal investigation for corruption in business practices, the German police seized several devices that the suspected person had used. The grand total of seized files was 14 million; the material that, after a thorough analysis, was printed out and attached to the trial dossier as relevant for the case amounted to 1.100 documents [27]. The situation is undoubtedly

---

[23] C-PROC, *The global state of cybercrime legislation 2013-2020: a cursory overview*, 20 March 2020, in *coe.int*, p. 5 ff.

According to the same source, 177 states have adopted or proposed specific substantive provisions for punishing crimes on computer systems or perpetrated by means of a computer system, prompting the Cybercrime convention committee's remark that «obviously, reforming procedural law and enacting specific procedural powers to secure electronic evidence for use in criminal proceedings (corresponding to Articles 16 to 21 of the Budapest Convention and subject to the safeguards of Article 15) is a more complex undertaking»: *The Budapest Convention on Cybercrime: benefits and impact in practice*, 13 July 2020, in *coe.int*, p. 6.

[24] See CYBERCRIME CONVENTION COMMITTEE, *The Budapest Convention on Cybercrime: benefits and impact in practice*, 13 July 2020, in *coe.int*, p. 5 f.

[25] With the notable exception of Spain: see L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, *infra*.

[26] O.S. KERR, *Digital Evidence and the New Criminal Procedure*, *Columbia Law Rev.*, 279 (2005), p. 279 ff.

[27] ECHR, 25 July 2019, Rook v. Germany; the case will be further analyzed later:

problematic for both privacy and proportionality, but this state of affairs is far from outlandish.

On the contrary, this way of proceeding is often (if not always) recommended by the technical standards: operating on a computer can lead to the modification, the erasure, the misplacement of relevant data, undermining the credibility of the entire operation. Moreover, it is often impossible to go through all the material on the spot: the sheer quantity of information that can be stored is always more difficult to navigate and master, also because data could be hidden in folders apparently devoted to private matters [28]. On the other hand, the choice of mirror imaging the entire memory instead of a selective acquisition could be dictated by the need to recover erased data, that leave a "latent" trace [29]; or by the presence of encrypted contents. A well-executed copy could allow for the preservation of the original set of data and can serve as matrix for more copies: the prosecution and the defense could perform their analysis on working copies, guaranteeing the repeatability of the operation.

The foundations of the digital investigation – gather everything, copy and analyze – appear to be in direct contradiction with the constitutional milestones on the collection of evidence, that ask to leave behind what is not strictly related to the case, and to impact on the person's right to privacy only insofar as necessary.

To be fair, sometimes the proportionality principle is respected after the copying of the entire data set: the research can be limited to the strict necessary only because there are not enough resources to extend it. However, this is not a satisfying counterbalance.

We are facing yet another paradox, and this time it is at the heart of the research we are presenting: if one wants to guarantee the reliability of the digital material, one will infringe upon the right to privacy; better protecting privacy means losing reliability.

The issue frequently occurs right in OLAF's domain: for example, one could need to examinate the informatic data stored on a corporate network, that could be shared with other branches and subsidiaries. A

---

see L. Bartoli-G. Lasagni, *Criminal and administrative investigations and digital forensics: a comparative perspective*, *infra*.

[28] N. Jones-E. George-F. Insa Mérida-U. Rasmussen-V Völzow, *Electronic evidence guide*, cit., p. 140.

[29] Circolare della guardia di finanza 2008, n. 1, *Manuale operativo in materia di contrasto all'evasione e alle frodi fiscali*, vol. II, available at *gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca*, p. 27.

complete acquisition would be very damaging to the corporations that are not involved in the investigation.

The legal layer of the considered systems rarely helps solving this conundrum, as it has been tailored on a different, factual situation: the rules were conceived to search for a specific object, find it and take it away; the selection was supposed to happen at the beginning and there is theoretically no procedure in place to sift out what is relevant, after the seizure happened.

But the problem has gained importance and, looking at other legal systems or at the relevant soft law, one could find many indications. For instance, when the relevance of the collected data is in doubt, OLAF's guidelines suggest to «place the forensic image in a sealed envelope and then invite the person whose data was forensically acquired for a meeting to conduct a preview of the device in his/her presence» [30].

In a case discussed at the European Court of Human Rights, the agents seized some hard disks and copied others; the target of the investigation was a lawyer accused of colluding with some of his clients to commit a crime. In front of the European Court, the Finnish Bar Association maintained that the police could have availed themselves of the procedure provided for in the Advocates Act, wherein the searched material would have been examined by an outside advocate who would have determined which material was related to the pre-trial investigation being conducted by the police and which was not [31].

This proposed remedy was liked by the Court [32], but it does not appear to be perfect. A lawyer that was never on that case before could struggle to identify the material's relevance to an investigation that he does not know in depth; moreover, during the investigation, when the fact has not yet been perfectly assessed, it might be difficult to establish a nexus of relevance; finally, a lawyer could not have the "investigative sensitivity" that could be necessary to the task.

---

[30] *Guidelines on Digital Forensic Procedures for OLAF Staff*, 15 February 2016 (available at *ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf*), art. 5.5. A similar solution also appears in § 6.3 if, «during an "On-the-spot check" of an economic operator, its representative claims that the device subject to the digital forensic operation contains data of a legally privileged nature».

[31] ECHR, 27 September 2005, Sallinen v. Finland, § 56.

[32] «The Court notes that the search and seizure were rather extensive and is struck by the fact that there was no independent or judicial supervision» (ECHR, 27 September 2005, Sallinen v. Finland, § 89).

DEVICES tried to add to this debate by elaborating workable, comprehensive proposals on the legal and technical side.

The topics are thorny; law enforcement agencies, lawyers, prosecutors, judges, are in search of some guidance; but they are not the only ones involved in the investigation. First responders often share the spotlight with experts, that come in as specialized practitioners or as consultants before or after the information has been secured. However, they would normally carry out the analysis and would give evidence in court, enjoying the elevated status of "scientist": their statements are normally trusted as epistemologically valid; nevertheless, their findings can only be as good as their training and their experience. That is why DEVICES has also been concerned with the national requirements for digital forensic consultants and, more generally, digital forensic experts: every state sets different standards regarding the training of in-house police experts as well as for private consultants; mandatory training requirements can have a tangible impact on the skillset that they acquire, and they vary from country to country; for instance, despite the growing need for digital forensic analysts, the Italian system still does not have a clear regulation in place.

Lastly, the research considered how the different countries monitor the storage and preservation of digital information for trial, and what precautions are taken to guarantee its integrity. The issue is not a new one: every piece of evidence presented to the court – digital or not – should be genuine; data, though, require a special degree of attention. DEVICES' results show an interesting convergence towards an American-style chain of custody, registering every change of hands, intervention, operation on the item. The traditional way of reporting would disperse the information in the dossier, whereas keeping it all on a single, dedicated document can improve traceability: the gaps are simpler to identify and the authenticity of the single piece of evidence becomes easier to assess.

Building trust between states is a long-term goal, one that a research project cannot hope to achieve, but deep changes do not happen in a vacuum. It is important to lay the groundwork to make cooperation easier, faster and more secure, especially in the domains where it is needed the most. Besides, in the era of expedited mutual legal assistance, of the fast exchange of digital material to be used in court, of European investigative bodies such as the European Prosecutor and OLAF, the discussion on the best way to reconcile the respect of the individual's fundamental rights and the reliability of a digital investigation is much needed. Hopefully, our contribution

will help in moving forward, towards a common, European notion of proportional and forensically sound digital investigations.

Raffaella Brighi-Michele Ferrazzano

DIGITAL FORENSICS: BEST PRACTICES AND PERSPECTIVE

Overview: 1. Introduction, issues, and goals. – 2. Digital forensics. – 3. Standards and guidelines. – 3.1. International standards and guidelines. – 3.2. Overview of guidelines, best practices and soft regulation of DEVICES' Partners. – 3.3. Guidelines on Digital Forensic Procedures for OLAF Staff – 4. Digital forensics expert: roles and skills. – 5. Main steps in digital investigations. – 6. The digital forensics lab: tools, facilities, and requirements. – 7. The big amount of data: technical requirements versus privacy. – 8. Conclusions: recommendation and perspective.

1. *Introduction, issues, and goals*

This contribution aims to conduct a technical investigation on the methodological requirements for the processing of digital evidence, with specific reference to anti-fraud procedures. In this context, from a digital forensic perspective, our research focuses on two aspects. The first one aims to identify the minimum criteria that need to be met in all the stages while processing digital evidence in order to obtain reliable evidence, as well as the skills needed by those who work on digital evidence and the characteristics required for the facilities (e.g. labs) entrusted with digital investigations. The second aspect relates to the amount of digital data that need to be gathered and brought to court in order to have meaningful evidence, while protecting the privacy of the individual in relation to the data stored in digital devices – this strictly related to the defence right of those who are subject to investigation. On this topic, the work sets out an alternative method for selecting the digital data, in such a way as to balance the two competing goals of ensuring complete investigations while respecting the privacy of those investigated, as provided by

the Guidelines on Investigation Procedures for OLAF Staff at § 15.3 [1].

In the practice of trial procedure, the peculiar structure of digital data engenders the illusion that what is digitally represented is indisputable, as is the meaning ascribable to such representation. This prompts us to uncritically believe that a digital exhibit is suited to support the judge's logico-probative reasoning.

Digital data is a representation that uses a binary sequence of bits that are not human-understandable. Therefore, it requires a series of operations through which a transformation is realized that may lead to different results (displayed as text on a screen or as a video, or again as an image printed on paper) [2]. Without interpretation, data cannot have any meaning [3].

By its nature, digital data is: "immaterial", requiring a suitable support to store on, such as a CD-ROM, hard disk, or flash drive; "volatile": it can easily be dispersed; "corruptible," meaning that it can be modified anonymously or involuntarily; "reproducible" without any limit on the number of copies that may potentially be made of it.

Digital evidence may be characterized as any data that (a) is allocated somewhere on a digital device or sent across computer systems of telecommunications networks and (b) can have some relevance in the outcome of a judicial process [4].

Every data useful to support or reject a theory about the way an

---

[1] Available at: *ec.europa.eu/anti-fraud/investigation-guidelines-olaf-staff_en*.

[2] For an introduction to the relationship between concepts of "data" and "information" see G. CONTISSA, *Information technology for the law*, Giappichelli, Torino, 2017, p. 73 ff.

[3] J. SOWA, *Conceptual Structures: Information Processing in Mind and Machine*, Addison-Wesley, Reading, MA, 1984.

[4] Both properties are included in the well-known definitions of digital evidence on which the technical-scientific community converges: the definition by the Standard Working Group on Digital Evidence – «Digital evidence is any information of probative value that is either stored or transmitted in a digital form»; and the definition by International Organisation of Computer Evidence – «Digital evidence is an information stored or transmitted in binary form that may be relied upon in court». A summary definition, which seems to cover every relevant aspect and also includes the concept of electronic evidence, was recently developed in the *European Evidence Project* (European Data Informatics Exchange Framework for Courts and Evidence, is a project financed by the European Commission as part of the 7th Framework Programme (Grant Agreement 608185)): «Electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using

offence was committed or to establish intent or an alibi can be considered digital evidence.

During a trial, the way digital data has been collected or stored is often challenged. This is owed to the fact that these activities necessarily require to deal with intangible material invisible to those with no specific competence in the area in question (an example could be a *log file* containing traces of illicit activity).

Neglect, lack of skill, or inappropriate methods can all result in the judge reasoning on data that have been misidentified or improperly collected or stored, leading to flawed expert opinions and reports.

As happens with any type of evidence, including digital evidence, the burden of demonstrating that the evidence is truthful and authentic falls on the party who introduces it. The use of digital evidence is constantly increasing, and it is therefore possible that courtrooms use, more and more, to keep copies of emails, digital photographs, word-processing documents, electronic spreadsheets, GPS tracking data, audio files, and digital videos.

Traditionally and historically, evidence has been presented either in tangible form (paper documents, printed photographs, and so on) or on the basis of witness or expert testimony. Digital evidence is obtained from devices that process digital data either locally (in the device itself) or within a computer network (typically the Internet). Like other kinds of evidence, digital evidence needs to be reliable and to preserve its integrity, meaning that it must be shown without alteration or tampering. Herein, then, lies the key challenge posed by digital evidence: because electronically represented data is intangible, it more easily lends itself to being altered or doctored than traditional sources of information, and these alterations are often difficult to perceive, detect, and document – all of which makes it necessary to use specific methods and technical procedures if digital data is to qualify as reliable and thus achieve the status of evidence proper.

Because recourse to digital evidence raises the issues that come up with scientific evidence, it becomes necessary to construct an epistemological framework [5] through which there is the need to define methodological standards and technical tools suited to

---

any electronic device. Digital evidence is that electronic evidence that is generated or converted to a numerical format».

[5] See S. Haack, *Legalizzare l'epistemologia. Prova, probabilità e causa nel diritto*, Egea, Milan, 2015; Id., *Six Signs of Scientism*, in *Logos & Episteme*, 3 (2012), i. 1, p. 75 ss.

guarantee the procedural certainty and transparency to cope with the increasing complexity of services in the ICT sector, as well as with the internationalization of investigations involving digital data.

Considering the foregoing, it will come useful to go through the list of the main characteristics by which digital evidence is distinguished:

intangibility: a digital bit does not present itself in any physical form, making it necessary to find for it an adequate support capable of storing so that it can subsequently be accessed;

alterability: digital data is binary (its value being either 0 or 1), making it possible to alter it anonymously, often without leaving behind any traces of such alterations, and as a result its processing needs to be done implementing appropriate measures by which to store and safeguard it;

change owing to regular use or mishandling: digital data can undergo change even as a result of "regular usage" (simply by booting up a computer), such that it is processing for evidentiary purposes needs to be subject to specific methods by suitably trained personnel;

volatility: once digital evidence is altered, it is no longer possible to restore it to its previously stored value; in addition, there are circumstances in which digital data can easily be dispersed owing to the characteristics of the support that stores it (consider, for example, the digital data contained in the RAM memory of a system that gets shut down while executing some process);

potentially unlimited reproducibility: any digital data can be copied to other devices with memory capacity, the only limit here being the amount of storage space available in these devices; it is worth noting, in this connection, that if a copy is made using the appropriate methods, it will not alter the original data, making it therefore possible to use copies that for all intents and purposes are originals.

2. *Digital forensics*

The aim of *digital forensics* [6] is to apply scientific and analytic

[6] On the subject: B.D. CARRIER, *Defining digital forensic examination and analysis tool using abstraction layers*, in *International Journal of Digital Evidence*, 1(2003), i. 4, p. 1-12; E. CASEY *Foundations of digital forensics*, in ID. (ed.) *Digital*

techniques to digital data stored on digital devices or moving across a digital network, so as to identify, process, and preserve such data, in such a way that it can be assessed as evidence at trial. Digital forensics thus answers the need for the technical and methodological rigor required by the legal process, and it defines best practices for managing digital evidence.

From the standpoint of digital forensics, any digital evidence needs to satisfy the following criteria [7] if it is to qualify as such:

integrity: this means that none of the activities done using the data can alter it, except where acquiring the data makes it necessary to resort to procedures that entail changes, which in turn will have to be kept to a minimum [8];

authenticity: digital data must present itself in the same condition in which it was originally acquired;

completeness: digital data needs to be acquired along with its context, in such a way as to make it possible to properly assess its probative value by either of the two parties concerned (those who bring it in as evidence in support of the claims they are making, and those who need to defend themselves against those claims);

reliability: digital data can not reveal itself to have been altered, and at any rate it must provide all the guarantees needed to forestall any doubt that may arise as to its authenticity and truthfulness;

pertinence: digital data needs to speak to the case for which it is brought in as evidence;

adequacy: digital data needs to be gathered in a manner that is

---

evidence and computer crime, 3rd ed. Academic, Waltham, 2011; L. DANIEL, *Digital forensics for legal professionals. Understanding digital evidence from the warrant to the courtroom*, Syngress, Amsterdam, 2012; J. HENSELER, *Computer crime and computer forensics*, in *The encyclopaedia of forensic science*, Academic, London, 2000; S. MASON, *Electronic evidence*, 3rd ed., Lexis Nexis Butterworths, London, 2012. See also M. POLLIT, *A History of Digital Forensics*, in K.P. CHOW-S. SHENOI (eds.), *Advances in Digital Forensics VI,* Boston, Springer, 2010, pp. 3-15. In Italy, one of the first definitions of the discipline and its scientific approach is presented in C. MAIOLI, *Dar voce alle prove: elementi di informatica forense*, in *Crimine virtuale, minaccia reale*, Franco Angeli, 2004 and in C. MAIOLI, *Introduzione all'informatica forense*, in P. POZZI (eds.) *La sicurezza preventiva dell'informazione e della comunicazione*, Franco Angeli, 2004. For an in-depth examination of the main areas of Digital forensics see also C. MAIOLI (ed.), *Questioni di Informatica forense*, Aracne, 2015.

[7] See, among all, E. CASEY, *Digital evidence and Computer Crime. Forensics Science, Computers and the Internet*, 3rd ed., Academic Press, 2011.

[8] In the Italian legal system, the acquisition of data susceptible to being altered in the process is governed by Article 360 of the Code of Criminal Procedure. See *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, §§ 2-3.

adequate to its purpose if its informational contribution is to be appreciable;

documentation: each step in the process needs to be documented in accordance with the *chain of custody* paradigm [9], following the lifecycle of digital evidence. That means that every step in the handling of digital data must be recorded chronologically, so as to make it possible to track and protocol the full journey the evidence makes from the moment it is identified to the moment it reaches trial, thereby guaranteeing a transparent process and the integrity of its outcome. Any expert, including an independent one or one the court appoints at a later time, needs to be able to repeat all the operations carried out during the digital investigation, and needs to be able to do so solely by looking at the chain of custody and having a copy of the data in hand.

It can be observed that in standardizing the manner of carrying out digital forensics operations, lawmakers across all countries have placed greater emphasis on the result that is to be achieved than on the method to be followed in working toward that result: the fear has been that if technical procedures are etched in the law itself, that would not have acted as a safeguard but, in the long run, would instead have led to contrary and distortion effects owing to the discipline's constant evolution and to the peculiarities distinctive to each case.

Until October 2012, the methods were set out in some sector-specific best practices aimed to outline the paradigms of technical procedure in digital forensics, this through a method that allows to (a) capture evidence without altering or damaging the original device; (b) authenticate the exhibit and the (bitstream) image [10] that

[9] To the need for documentation, the *best practices* give an answer with the North American institute, already used for particular types of physical goods, of the "chain of custody". This term alludes, in our system, to a complex of procedural rules and technical regulations which – with the ultimate aim of guaranteeing the genuineness and integrity of the finds and the traceability of the operations – impose the meticulous documentation of every step taken by the digital data from the moment of acquisition to their entry into the process. On this subject, see L. BARTOLI-C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, 2015, i. 1-2, p. 139-151. On the implementation of computable models for the chain of custody, please refer to R. BRIGHI-V. FERRARI, *Digital evidence and procedural safeguards: potential of blockchain technology*, in *Ragion Pratica*, 50 (2018), i. 2, p. 329.

[10] A bit stream image (or a forensic copy, or bit-to-bit copy) is the bit-by-bit copy of digital data in one digital data storage device to another digital data storage device, either in clone mode or in image mode. With this methodology, exact cloning is

has been captured; (c) guarantee that the findings of fact can be repeated; (d) analyze the original data without modifying it; and (e) ensure that the fact-finding activities are as impartial as possible.

From the standpoint of digital forensics, then, the digital nature of the evidence makes it necessary to take two elements into account.

(i) The first is an *objective element*, and it consists in following sector-specific standards and guidelines. There is a twofold criterion that is doubtlessly useful in enabling information technology to effectively interface with the law: for one thing, the chosen standards should not force the use of any specific technology that practitioners must commit to indefinitely; and, for another, the operating procedures and investigative methods supported by the standard must be ones in wide use among digital forensics experts.

(ii) A *subjective element*, consisting in the skillset the forensics expert applies to digital data from the moment the digital evidence in question is detected. This is an essential element, considering that a legal proceeding can be seriously undercut by ignorance of the duties and responsibilities assumed under the law governing the handling of digital data, and considering the legal consequences of mishandling such data, as well as by failure to use the techniques the law prescribes for such handling.

In practical terms, however, the development and implementation of common procedures comes up against two limits, one having to do with technology – particularly as concerns the media on which data is stored and the "technological habitat" in which the device in question works and is put to use – the other owed instead to the subjective element, meaning the subjectivity that individuals bring to their activity, as well as the aims pursued through that activity: for law enforcement, the aim will be to acquire the elements needed to advance their investigation, all the while preserving the authenticity of the evidence so acquired; for the judiciary, the aim will be to connect those discoveries to criminally relevant facts; for the court-appointed or party-appointed expert, the aim will be to check that the procedures followed in obtaining the evidence at hand are consistent with a proper exercise of the right to defence.

---

performed without loss of data in the destination and without alteration of data in the source. See below, § 5.

3. *Standards and guidelines*

Digital forensics experts have several guidelines at their disposal, each laying out principles and methods for the proper handling of digital evidence.

In order to provide technical and methodological rules for the collection and the handling of digital evidence in antifraud procedures, the research was focused on: (a) the selection of the main international standards and guidelines, in view of the international recognition they have gained and of their relevance to antifraud, (b) the overview of guidelines and best practices recommended by partners, and (c) the exam of *Guidelines on Digital Forensic Procedures for OLAF Staff* (2016), treated as a point of reference for the final recommendations.

3.1. *International standards and guidelines*

The main international standards and guidelines, selected in view of the international recognition they have gained and of their relevance to antifraud, are the following.

ISO/IEC International Standards. Since 2012, the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) have put out technical standards forming a coherent corpus serving as a useful reference point for digital investigations in all areas in which such investigations occur. These standards therefore cover not only criminal but also civil procedure, as well as investigations carried out internally within government agencies and private organizations alike, and whose findings may therefore never end up in a courtroom. ISO standards are (i) international, (ii) independent of the law in force in each single country, and (iii) independent as well of the instruments and technologies that may be used in complying with them (*technical neutrality*). In particular, the ISO/IEC standards relevant for the purpose of this research are the following: (1) ISO/IEC 27037 «Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence»; (2) ISO/IEC 27041 «Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method»; (3) ISO/IEC 27042 «Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence»; (4) ISO/IEC 27043 «Information technology – Security techniques – Incident investigation principles

and processes»; (5) ISO/IEC 27050 «Information technology – Security techniques – Electronic discovery».

Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI, 2015). The European Network of Forensic Science Institutes (ENFSI) [11] was Established in 1995. Today it comprises 37 European countries, including most of the EU member states. As a network of experts, ENFSI is devoted to the purpose of sharing knowledge and experiences and coming to mutual agreements in the field of forensic science, including the domain of digital evidence. For this purpose, the ENFSI encourages all the laboratories that are part of the network to comply with best-practice and international standards in order to ensure quality and competence. The Best Practice Manual (BPM) for the Forensic Examination of Digital Technology (2015) provides frameworks for procedures, quality processes, and training processes for forensic examinations in IT. It is focused on providing guidance for forensics laboratories having to comply with international and local regulatory standards. Particularly section 4 defines the characteristics an IF laboratory needs in compliance with the ENFSI code of conduct. It sets criteria for (i) the composition of the digital forensics unit (section heads/operations managers, technical experts; analysts, assistants), (ii) the equipment, (iii) the reference material, (iv) the workplace setting and environment; and (v) the archival practices. The BMPs addresses all the phases of digital investigations, from the methods for handling items (physical seizure, protection, the transportation and archiving of digital evidence), through to the case assessment and the examination and reconstruction of events, and including the evaluation, interpretation, and presentation of findings.

Electronic Evidence Guide (EEG, Council of Europe, 2013). The Electronic Evidence Guide (EEG), developed by the Council of Europe, is intended for use by law-enforcement and judicial authorities only to support and guide them in identifying and handling electronic evidence using methods that will ensure that the authenticity of evidence will be maintained throughout the process. The EEG has been prepared with a special focus on the fight against cybercrime. It also covers state-of-the-art technology such as mobile

[11] ENFSI is the EU's regulatory agency that sets the standards to be used in forensics labs. Its operating protocols are therefore in use by Europol as well as other EU agencies doing forensic work. A list of associated laboratories may be found at *enfsi.eu*.

devices and cloud storage and has a section on live-data forensics, raising awareness of how important it is to be able to capture volatile data.

Electronic evidence: A basic guide for first responders (ENISA, 2014). The guidelines issued by the European Union Agency for Network and Information Security (ENISA) [12] have been developed with a view to supporting and shoring up collaboration between Computer Emergency Response Teams (CERTs) and law enforcement, and are designed to help CERTs in their task of supporting law enforcement in gathering evidence. To this end, the guidelines integrate the welter of material that exists on the topic of digital forensics, often written from a law-enforcement perspective, so as to provide CERTs with guidance in an area that is often new to them, in such a way that they can deal with potential digital evidence and the evidence-gathering process. The guidelines touch the different phases first responders encounter when performing digital forensics or electronic evidence gathering and describe how they should act before and while arriving at the scene, what they should keep in mind when performing memory forensics, etc. Then, a CERT first responder can deal with gathering of electronic evidence in an appropriate way and have a good communication with law enforcement.

Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019). The Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings (2019) [13] are the first international instrument designed to address issues arising in specific relation to electronic evidence in civil and administrative proceedings. Like other international standards for the handling of digital evidence, these guidelines deal with the use, collection, seizure, transmission, storage, and preservation of digital evidence. They also address awareness-raising, training, and education. It is worth pointing out § 4 of these guidelines, with their emphasis on due process rights [14].

---

[12] Electronic evidence: a basic guide for first responders (ENISA, 2015), online at *enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders*.

[13] Online at *search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c*.

[14] On this subject see *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 4.

Particularly relevant are the following guidelines, developed at the national level, but widely turned to at the international level as well.

Guidelines on Digital forensics (NIST – National Institute of Standards and Technology, USA, 2014). The NIST [15] Guidelines on Digital forensics [16] (2014) provide basic information about digital devices and forensics tools designed for the preservation, acquisition, examination, analysis, and reporting of digital evidence stored on digital devices. They primarily focus on mobile devices, including personal digital assistants (PDAs), smartphones, and tablets with cellular-voice capabilities. They are intended for forensic examiners, response-team members handling a computer security incident, and organizational-security officials investigating employee-related incidents. They assume a working knowledge of traditional digital forensics methods.

Good Practice Guide for Computer-Based Electronic Evidence (ACPO – Association of Chief Police Officers, UK, 2012). The ACPO guideline Good Practice Guide for Computer-Based Electronic Evidence (2012) is primarily written for law-enforcement personnel who may need to deal with digital evidence. This guideline was first released in the late 1990s. Since then, there have been five iterations; some of the changes include an update in document title. The guide is essential reading for anyone involved in the field of digital forensics. The latest version has been updated to include more than just evidence from computers. It sets out some shared principles as follows:

Principle 1: no action taken by law-enforcement agencies, persons employed within those agencies, or their agents should change data which may subsequently be relied upon in court.

Principle 2: in circumstances where someone finds it necessary to access original data, they must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: an audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: the person in charge of the investigation has overall

[15] NIST - National Institute of Standards and Technology, USA.
[16] All guidelines are available on NIST website *nist.gov*.

responsibility for ensuring that the law and these principles are adhered to.

Particularly relevant for our topic here is § 7.1, addressing "Training and Education". The guidelines underline that training in digital investigation significantly differs from usual police training. Owing to the rapidly changing environment of technology, there is a requirement for the continuous but essential retention and updating of skills [17].

3.2. *Overview of guidelines, best practices, and soft regulation of DEVICES' Partners*

The analysis of *National reports* from DEVICES' Partners points out that international standards are the common reference base for professionals who work in digital forensics area. Some countries (or better, local law enforcements, agencies, or corporations) recognize them in local guidelines or soft rules, others do not.

In Spain [18], Law enforcement agents (LEA) in the criminal investigation and IT experts in private digital investigation (for companies, for labour proceedings, for internal investigations within the obligations set out in CCL compliance programmes, etc.) follow the same protocols, guidelines and standards, and mainly the UNE standards, [19] which are certified by AENOR (Asociación Española de Normalización y Certificación), very similar to ENFSI and ISO international standard. All forensic analysis requires a quality control of the acquisition of the data or samples that will be subject to forensic analysis, which implies the traceability of the chain of custody. Within the UNE standards, there is a detailed description on what are the processes and information to be checked at the examination stage and reflected in the report. The standard describes a list of data, actions and processes that should be included, although the list does not pretend to be exhaustive: the practioner can collect other data and perform other actions. Further the information provided by the relevant police unit (*policía científica*) to Project's partner National legal expert confirms that they prepare

[17] See below § 4.

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

[19] UNE is the acronym for Una Norma Española. UNE is in fact an ISO member standardisation body.

their reports and expert opinions following the already mentioned standards.

In Germany [20], at the federal level, a standard for digital investigations have been set with the Guidelines on "IT forensics" by German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik-BSI). The guidelines explain the use of IT forensics and are designed both as a basic guide, which allows a deeper understanding of the matter, and a reference work for the solution of practical problems. The guidelines are mainly addressed to system operators, i.e. the private corporations. However, the principles established within the guidelines and a part of their contents are relevant also for law enforcement investigations in State Criminal Police Offices. Furthermore, the BSI Guidelines are the main reference work for defence lawyers to challenge digital evidence. The various State Criminal Police Offices follow also standards based on guidelines adopted by the respective authorities (not public). Guidelines may also exist for the prosecution services, which again may differ widely among institutions.

In Italy [21], the main standard in use by LEA and by IT forensics Expert of private company are ISO standards and the other international guidelines mentioned in § 3.1. The Guardia di Finanza (or GdF) – a militarized law-enforcement agency under Italy's Economy and Finance Ministry responsible for dealing with financial crimes and smuggling – produce the circular n. 1/2018, an internal document released on the agency's website, [22] entitled «Operating Manual on Tax Evasion and Tax Fraud» and runs to 1,251 pages across four volumes. It has introduced the role of the "Computer Forensics and Data Analyst" (CFDA), a qualified practitioner responsible for identifying, collecting, and acquiring digital evidence. GdF provides specific training for first responders, this in keeping with international standards in digital forensics like ISO/IEC 27037 – Annex A.

Finally, the Dutch and the Luxemburgian [23] National Reports do

---

[20] See *infra*, S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 3.2.2.

[21] See *infra*, L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, § 2.

[22] Available at: *gdf.gov.it/documenti-e-pubblicazioni/circolari/circolare-1-2018-manuale-operativo-in-materia-di-contrasto-allevasione-e-alle-frodi-fisca*.

[23] See *infra*, K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxemburg*, § 1.

not recognize any specific (public) guidelines, or soft regulation or checklist of operation carrying out digital investigation.

3.3. *Guidelines on Digital Forensic Procedures for OLAF Staff*

The relevance of OLAF investigations in the European antifraud legal framework, coupled with OLAF's close cooperation with national authorities, makes the *Guidelines on Digital Forensic Procedures for OLAF Staff* (2016) the starting point for our study on the development of common standards for digital investigations in the EU and a term of comparison for all the involved Member States.

These guidelines, issued by the European Anti-Fraud Office (OLAF), are intended for use by its staff for the purpose of identification, acquisition, imaging, collection, analysis, and preservation of digital evidence. The aim of these Guidelines is to establish rules for conducting digital forensic operations in a manner that ensures the integrity of the evidence and of the chain of evidence, so that the evidence may be admissible in administrative, disciplinary, and judicial procedures.

These guidelines are modelled on ISO and ACPO technical standards, but taking a dual approach, at once technical and legal. In this respect the OLAF Guidelines stand apart from strictly technical standards, in virtue of their relating the technical requirements to the specific EU provisions in which they find their legal basis.

Due to the fact that these guidelines do not merely regulate the technical aspects of an IT investigation, OLAF's guidelines provide for the involvement of various professional staff: the first is the investigator, who is generally responsible for conducting the investigation and is familiar with the legal aspects; then, the involvement of the Digital Evidence Specialist (DES)[24] is also required, who is permanently integrated into OLAF's staff and has specific technical knowledge in the digital field. Further actors may be involved in the digital investigation, including the Legal Advice Unit, the consultant of the subject concerned by the investigation, and the (possible) national authorities involved. There is a clear separation of roles between the investigator and the expert who deals with the management of the IT data, which also means the setting

[24] Competence, skills, and role of the digital evidence specialist is examined in depth in § 4.

up of standard models for the discussion between the IT expert and the investigator.

The guidelines describe the sequence of operations that DES has to perform (see below, § 5), from the identification of potential digital evidence to the acquisition and transport to analysis activities, in accordance with the main international technical standards but discounting, compared to the latter, the lack of a certain technical precision. OLAF's operations are characterized by the drafting of specific Reports [25], i.e. summary documents containing the activities carried out relevant for the preparation of an accurate chain of custody. During investigations, a file (*case file*) is kept up to date through an information system called Case Management System, which tracks all the actions taken, the operators involved, and the information collected.

OLAF also has a forensic laboratory where forensic analysis activities take place (see below, § 6). The data collected by DES are transferred to the servers of the forensic laboratory and constitute the so-called "forensic work file", a file that is stored on the laboratory server for the time necessary to carry out the investigations.

For analysis, the investigator must submit a request to DES about the subject of the data search; he cannot require an indiscriminate apprehension of the data without stating a logical criterion to guide the choice of what to extract and what not.

DES will only provide those files that match the Investigator's query: all other data will be stored on the server and will not be visible to the Investigator. The step is of crucial importance, and from an organizational and technical point of view it represents a remarkable step forward, totally unparalleled, for example, by our system. DES shall also prepare a separate Report, called the "Digital Forensic Examination Report": it summarizes the results of all the operations carried out by DES, and lists all the information provided to the Investigator as a result of the analysis. The Digital Forensic Examination Report will also be included in the investigation file (CMS casefile).

In conclusion, the guidelines provide both for the compliance with specific technical measures and the provision of adequate facilities, as well as the guarantee of the legal requirements of proportionality.

On the technical side, however, we cannot fail to point out that

[25] Digital forensic Operation Report, Digital forensic examination report and the Operational Analysis Report.

although the OLAF guidelines are in compliance with the main technical reference standards, they lack technical precision and accuracy in several steps (see in this respect below, § 5). Technical integration is necessary because they do not tell us how DES should proceed in practice, nor which programs she should use, but this is left to other sources that are not mentioned. On the other hand, the aim of the guidelines is not to provide an accurate technical manual to inspire the work of DES (as EEG or ENSI guidelines) nor to indicate in general the technical objectives to be achieved (as the ISO/IEC standards): The aim is to show to the investigator the limits imposed by technology, and to DES the aims and safeguards that the law requires of his work. In short, the guidelines are that common knowledge hub that technicians and jurists should jointly know, without prejudice to the specific areas of specialist knowledge that each maintains.

4. *Digital forensics expert: roles and skills*

International technical standards, as well as many best practices developed nationally, insist on the importance of the technical personnel entrusted with digital forensics activities, devoting specific sections to defining roles and skills for such personnel. The required degree of technical skill is high, and it needs to be rounded out with an understanding of the applicable law if these technicians are to be able to properly handle digital evidence. Availability to advanced IT tools is not sufficient.

The ISO/IEC 27037 standard singles out two professional figures: the Digital Evidence First Responder (DEFR) – an «individual who is authorized, trained and qualified to act first at an incident scene for handling digital evidence» – and the Digital Evidence Specialist (DES), whose preparation is normally deeper and more specific in comparison with the DEFR, and who may «handle a wide range of technical issues». In addition to providing a specific table with the different skills required for different purposes (Annex A, ISO/IEC 27037), the standard underscores on multiple occasions that practitioners need to have technical as well as legal training. It is up to each jurisdiction to define the criteria required to qualify as a DEFR or a DES, and in these roles, practitioners need to demonstrate the ability to do investigative work (sec. 6.4 ISO/IEC 27037).

Even greater specificity can be found in the ENFSI guidelines,

according to which forensics experts mut be tested regularly to assess their ability; also laboratories are regulated more strictly and are periodically reviewed with regard to the quality of the tools and their adequacy.

ENFSI places emphasis on testing not only the theoretical understanding that practitioners have of the subject matter, but also their practical, hands-on abilities, which is done by giving them a simulated IT problem that they are then asked to solve.

Under the impulse of international standards, some local authorities have defined the role and skills of personnel authorized to work in digital investigations.

The ACPO guidelines highlight that the general principle for training in digital investigation differs significantly from the principle governing police training, in which connection it refers us to the *ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation*.

In Italy, GdF Circular n. 1/2018 introduced a specific figure, qualified and trained in Computer Forensics and Data Analysis (CFDA). Professionals in this role are part of the staff of the judicial police, and they are uniquely qualified to acquire and analyze digital evidence, access the data of multinational groups that share data across branches. Owing to the peculiarities a tax audit involves at the initial phase, in which digital evidence is acquired and assessed, the GdF General Command has also launched courses designed to train first responders in line with the international standards covering the same subject matter.

The National reports by the Legal experts involved in DEVICES' Project show that if digital evidence is important for the case and special analytical expertise is necessary, technical operations and analysis may be carried out by special IT forensics Units within the LEA (e.g. the IT Forensics Unit of the *Policía científica* in Spain)[26]. Police officers who want to specialize in IT forensics may get additional training and qualifications. Training is refreshed and competences re-assessed periodically. In the Netherlands specifications on the training and the necessary expertise are given in a Ministerial Decision. Specific training courses and certifications

[26] See *infra*, L. BACHMAIER WINTER, *The handling of digital evidence in Spain*, §§ 2-3; L. BARTOLI-G. LASAGNI, *The handling of digital evidence in Italy*, §§ 2-3; S. GLESS-T. WAHL, *The handling of digital evidence in Germany*, § 3.1; K. LIGETI-G. ROBINSON, *The handling of digital evidence in Luxembourg*, § 2.

are required, for example, to identify system weaknesses and to modify codes in order to access automated systems (OSCP) and to collect data from wireless networks and circumvent the restrictions of these wireless networks (OSW). Members of the technical team must possess some legal knowledge as well. Although there is no strict separation between a DEFR and a DES, the police officer who is present at the "acquisition" phase (regularly a seizure of an object/of data) is usually different from the one who does a "technical analysis". In Germany and in the Netherlands the specialists at the special units are not handling the case, i.e. they do not make conclusions on the analyzed data. Their work is more or less limited to "data preparation", but the investigator handling the case has to choose what data need to be processed.

The OLAF Guidelines likewise provide that a digital investigation should always involve a professional specifically trained in digital forensics: this is the Digital Evidence Specialist (DES), a member in the OLAF staffs bringing «specialised technical expertise to perform digital forensic operations and to prepare related reports». The DES supports the investigator, who leads the investigation, is responsible for it, and knows all its legal implications. The OLAF Guidelines prohibit the investigator from interacting with anything that may prove useful as digital evidence, so much so that if anyone should come forward with a device on their own accord, the inspector may not accept it. Only the DES is authorised to do so and to copy the contents stored on a device; this in order to avoid tampering and to preserve the chain of custody. On the other hand, DESs may only be involved in the digital operations that fall within their purview, and they are neither acquainted with the broader investigative context nor are they to take any interest in the concrete case at hand. As we will see, this can prove limiting if the need should arise to accord priority to certain operations over others or to select the material that is relevant to the investigation.

It should at any rate be observed that because OLAF is equipped with its own investigative tools, it is fully compliant with the applicable technical standards, and it is also in a position to audit its own work.

It should further be underscored that the periodical quality check improves if carried out by internal personnel, that are part to the same administrative structure. This is an added value because OLAF does not need to rely on external experts and practitioners that may not have the same experience with the justice system and with OLAF's work.

Digital forensics operators in Italy are a broad and diverse group today, with professionals whose training varies considerably, and some may even not have the skills necessary for the role that is entrusted to them in a trial. The problem lies in the fact that there is no specific job qualification, making it possible for anyone to enter the job market even with a rudimentary understanding of the subject matter.

Here we report some data providing a snapshot of the Italian landscape in this regard. In light of the data provided by ONIF (the country's National Digital Forensics Observatory), 72,6% of legal forensics consultants hold a higher-education degree, and only 40,3% of those in this pool hold a degree in information technology or a related field. As concerns training and continuing professional development, 45% has not gone completed any specifically designed university programme, 78% has no professional certification in the field. More than that, the tools of continuing professional development in large part consist of a combination of textbooks, dedicated websites, mailing lists, and social networks, thereby stripping the training down to its bare minimum. As for professional bodies, 53% of digital forensics experts are unregistered, either because there is no such specific body or because there are no degrees through which to gain access to the profession, as is the case with some programmes offered under the old curriculum. The professional body with the highest number of registered members is the engineering society. Of all interviewees, 42% were registered with an association of expert witnesses for the court in whose jurisdiction they were working, but there were also cases in which someone might be registered with more than one court – an option that the law does not in theory allow. Only 30% of the professionals interviewed were covered by professional liability insurance – although, to be fair, there is no legal requirement to obtain such coverage [27].

The National reports of DEVICES' Legal experts show that in other countries some level of quality is ensured by professional associations or lists of computer forensic experts. In Spain, the expert evidence presented by the defendant or any other private party in the criminal procedure needs to be prepared by an IT expert with the relevant training and registered in the official association. These associations are public institutions guaranteeing the

[27] ONIF Survey 2015, *La professione del consulente tecnico informatico in Italia*, Rome, 28 April 2016, *onif.it*.

professional quality/degrees and standards, both technical as deontological [28]. In Germany, if a court or public prosecutor wants to appoint an expert (*Sachverständiger*), they can resort to lists of experts provided for by the Chamber of Industry and Commerce (IHK). A certification of the expertise is not required by law. Bigger firms have, however, a certification by the German Federal Office for Information Security (BSI) [29]. There is no register for digital forensics experts in Luxemburg, but the website of the Luxembourg Ministry of Justice maintains lists of experts assermentés, with a handful self-described as specialising in IT and/or cybercrime [30].

The best setting, however, seems to be the Dutch one: the Register of Court Experts (NRGD) guarantees and promotes the quality of the contribution that court experts make to the legal process, and it could well serve as an example to other legal systems. The NRGD was the first register of forensic experts, established under the Experts in Criminal Cases Act of 2010 and managed by an independent Board of Court Experts. Although anyone can work as forensic expert even if they are not registered in NGRD, the registration gives experts recognition.

From the foregoing analysis of existing standards and experiences we can distil the following essential characteristics that anyone should embody in the role of forensic expert:

a capacity to do the job in a manner that is independent, impartial, conscientious, competent, and trustworthy;

proper and transparent conduct in relating to all the parties who have a stake in the case at hand;

an ability to communicate competently with all the other parties involved in the proceedings in a professional role;

confidentiality in using the data and information that one gains access to over the course of an investigation, in keeping with all applicable laws;

constantly staying up to date by completing training programs, attending conferences and seminars, and reading the literature (books, papers, journal articles, blogs);

using tools and techniques which the scientific community recognizes as suited to the task of acquiring digital evidence and guaranteeing its integrity, in compliance with all applicable laws;

---

[28] See L. BACHMAIER WINTER, *National Report: Spain*, § 4.

[29] See *infra*, S. GLESS-T. WAHL, *National Report: Germany*, § 3.1.

[30] See *infra*, K. LIGETI-G. ROBINSON, *National Report: Luxemburg*, § 2.

using proven scientific methods, or other methods whose reliability can be verified, when analyzing or interpreting data (e.g., verifying results by using different methods or using accepted datasets when establishing correlations between different data points), all in keeping with applicable laws;

applying the methods that international guidelines set out for the most common activities (e.g., search and seizure, transfer of devices, data acquisition) and for best practices concerning all activities in which it proves impossible to guarantee that evidence will not be altered (e.g., data captured from smartphones or from systems with a running task), all in compliance with the law;

the ability to properly handle situations for which there are no well-established practices and techniques (e.g., when dealing with data stored on remote devices, or on an Internet server, or on non-standard devices), an ability that will have to be maintained by hands-on experience and by continuously keeping up to date on the latest developments in the field;

the ability to provide clients with verifiable reports (whether oral or written) fully and clearly explaining the basis for the task that needs to be assigned, as well as any other aspect of one's personal experience and background which may be pertinent to the same task.

Finally, it is worth mentioning the question of the digital forensic expert's relation to service providers: the seizure of data from the latter bypasses almost all of the technical and methodological guarantees set out in international standards, for it is entirely up to the service provider to guarantee the quality of the data it collects and hands over to the authorities.

5. *Main steps in digital investigations*

On the basis of the standards that have been considered in this research project, we can identify the main steps of the digital investigation process.

Digital investigations are defined as the «use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while [...] preserving digital evidence, and maintaining the chain of custody» (ISO/IEC 27043). It comprises several steps and two main phases (Figure 1).

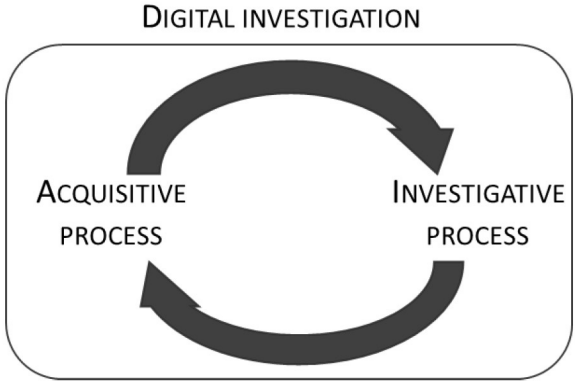

Figure 1 – Digital investigation process

Its two mains phases consist of the processes of (Phase one) acquiring data and (Phase two) using it for an investigation. The output of the acquisition process is input for the investigative process. Sometimes, the output of investigative process can suggest other activities that require a new acquisitive process. And so on, until the end of the investigation.

"Phase one" is the Digital Evidence [initial] Handling Process, which includes identification, collection, acquisition, and preservation of potential digital evidence. As the name suggests, the acquisition process is the process through which data is acquired or captured. In the OLAF guidelines, this is referred to as the "digital forensics operation", which the Digital Evidence Specialist (DES) carries out using forensic equipment and software tools. Its aim is to locate, identify, collect, and/or acquire and preserve any and all data which may be relevant to an investigation, and which may be used as evidence in administrative, disciplinary, or judicial procedures.

"Phase two", investigative process (which the OLAF guidelines call "operation analysis"), is concerned with analyzing the evidence, interpreting the results of the analysis, reporting the results of the interpretation, and presenting these results in a court of law, with the use of specific analytical tools and techniques by which to establish links between pieces of information.

Each phase is composed of steps (Figure 2) that must be sequentially followed in each digital investigation.

However, there are some precise factors that require a case-by-case assessment of the operations to be performed. These factors include the following: the digital device is turned on or off; the system cannot be removed because it provides a critical service or

because it is in the network and therefore cannot be physically reached; legal reasons why the digital device may not be acquired.

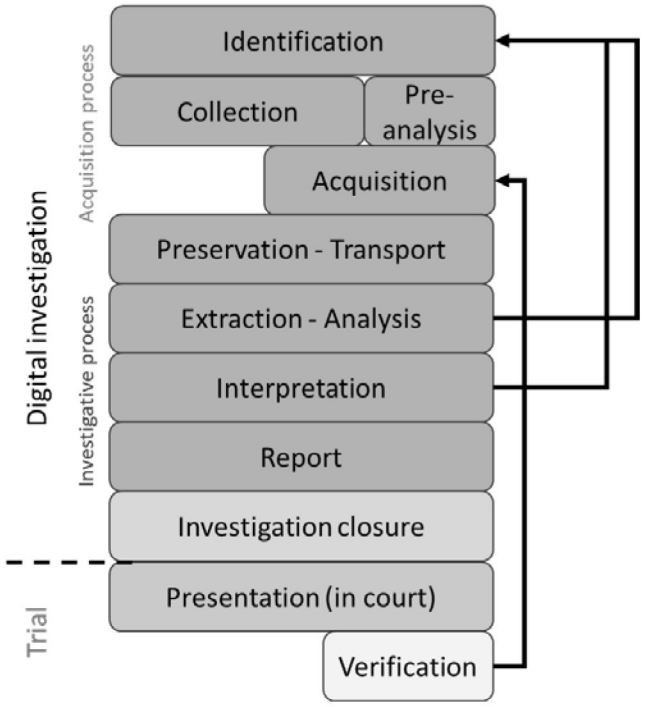

Figure 2 – Main phases of a digital investigation

The acquisition process comprises five main steps, in which the digital evidence is (1) identified, (2) collected and sometimes preliminarily analyzed, (3) acquired, (4) preserved, and (5) transported.

A point of discussion about this process is the one related to its repeatability: all of these steps are particularly critical because any mishandled operation in this phase could cause data to be altered or lost along the way, thereby making it impossible to verify or repeat the results of the investigation.

All the technical standards require that a complete and accurate record must be kept of each operation, even by photographing or filming the activity.

In terms of protection of the chain of custody and documentation of the activities, it is also necessary to highlight the EEG guidelines that require the documentation of the scene on which the IT technicians operate, as well as photos and videos to trace the state of

computer systems at the access. If possible, a 360° recording of the environment can be useful.

By that, all the activities, movements, and choices operated by the technicians are implicitly documented, so this substantial documentation can well support the accuracy of the acquisition process.

In the same direction, the ISO/IEC standards suggest documenting by any means possible both the status of the places prior to the operations and the procedures for completing the operations [31]. Also, the ENISA guidelines clearly indicate the obligation to register and document the performance of the activities [32].

The first activity, as mentioned, consists in identifying potential digital evidence. The Digital Evidence First Responder (DEFR) or Digital Evidence Specialist (DES) should search for items that may contain digital data relevant to the incident: computers, devices (scanner, printer, GPS tool), storage media, and networked devices [33].

This is not a simple task: physical devices or virtual spaces must be identified (as cloud-computing repositories). The devices can also be very small. The DEFR needs to also look for power cables, SIM cards, etc. If the DEFR does not identify the data correctly, it may thereafter never be recoverable.

In identifying data (step 1), the DEFR should establish priorities in the collection or acquisition of potential digital evidence, this depending on how volatile the data is and on its relevance to the investigation. In this case, however, who is carrying out IT activities must grasp the reason why the evidence is being collect or acquired. The OLAF Guidelines make it a requirement to exclude all data that is not relevant to the investigation.

The next step (2) is to decide whether to collect the digital devices or acquire the digital data. Collection is the process of removing electronic devices from their location and taking them to a forensics laboratory in order to subsequently make a forensic copy. The entire process needs to be documented from packaging to transportation.

Acquisition (step 3) involves creating a copy of data and

---

[31] ISO IEC 27037 par. 6.2.1; par. 7.2.1.2.

[32] Par. 2.1.2, *Digital forensics Handbook, Document for teachers* (ENISA), September 2013, available at *enisa.europa.eu*.

[33] For a practical guide on technical aspects see, among all, D.R. HAYES, *A Practical Guide to Digital Forensics Investigations*, 2nd ed., Pearson, 2021; B. NELSON-A. PHILIPS-C. STEUART, *Guide to computer forensics and investigations*, 6th ed., Cengage, 2018.

documenting the activities performed. The DES can make an image copy or clone [34] using dedicated software [35] or dedicated hardware [36]. All best practices require at least two copies in order to ensure that no physical damage is done to hard drives or logical damage to data.

Best practices require verifiable copies using hash functions of all bits contained within each media item. The DEFR should use the most appropriate method.

Returning on the technical gaps in the OLAF guidelines, it is worth pointing out that they do not indicate an order of priority for the acquisition of digital media, even if all international standards do so. For example, RAM must be acquired before non-volatile data: this is a common rule, shared by any standard as well as by the scientific community.

The ISO/IEC 27037 standard dedicates an entire paragraph to the topic of acquisition priorities of digital evidence.

The EEG guidelines do not directly express priority rules, but they clearly favour the prioritization of the volatile data, since they impose not to turn off a turned-on computer.

Moreover, OLAF guidelines do not suggest the usage of the least invasive software for the acquisitions [37].

The main criteria to collect or acquire data, dictated by international standards, include: the volatility of potential digital evidence; encryption applied to an entire disk or volume where passphrases or keys may reside as volatile data in RAM memory or in external tokens; legal requirements; resources such as storage size, availability of personnel, and time limits; the ability to seize a device.

---

[34] The bit-stream copy by clone is a mechanical copying of the single bits to a blank target support, creating a perfect clone of the source. In the imaging copy process, a file (or a set of files) is created and it represents the exact sequence of bit, useful to reconstruct the source. The main pros of the image are the possibility of making multiple copies on the same target, as well as the usage of a compression algorithm that reduces the disk usage.

[35] This kind of software includes dd Linux command or commercial products like FTK Imager, Encase, and Xways.

[36] Complete acquisition in over a short period can be accomplished by forensic duplicators like Tableau TD3 and Logicube Falcon. These are fully featured, fully forensic duplicators that offer an ideal combination of ease of use, reliability, and ultra-fast forensic imaging of hard disks and solid-state drives.

[37] The EEG guidelines demand (§ 3.4.2) the usage of the less invasive software, suggesting one instead of others, because of the less memory requirement for the execution.

In this context, a pre-analysis will often be carried out in order to identify the data that may be relevant.

During pre-analysis, some operations may damage the original data, and the verification process cannot be performed. That is made up for by photographically documenting the activity and providing a basis for each choice. The practitioner should be able to explain the effects of any actions taken.

Generally, technical standards require that all data stored on all devices be integrally captured (by making a copy of the entire image), for it is only by looking at how the single data point is consistent with the rest of its data environment that it may be determined whether the data has been altered. In some circumstances, partial or selective copies of the data are allowed, as for example when the quantity of the data to be captured makes it impracticable to capture the entire image on a hard disk. However, where this latter method is used, investigators need to be sure that all relevant data has been captured. In short, the rule is: seize everything, capture the data partially only when technical constraints do not allow for the complete collection. At the same time, the law requires that the personal sphere of those under investigation be encroached upon as little as possible, while refraining from capturing whatever data is not strictly necessary to establish the facts.

We should point out that the OLAF Guidelines do not permit the collection of physical devices, so what the DESs should do instead is only make copies of the data that is stored on them. Moreover, DES can analyze in preview data to decide if she must acquire all data, some data or nothing, according to the investigation requirements.

The issues related to the balance between the principle of proportionality and technical requirements for completeness are the subject of the next section.

The last two phases (step 4 and step 5) in the acquisition process concern the methods of transporting and storing the devices and the copies acquired, as well as maintaining and safeguarding the integrity and original condition of potential digital evidence, so as to be able finally to analyze the evidence.

The OLAF Guidelines require data to be stored in the CSM case management system in the forensic laboratory. This repository must follow robust security policies.

We can conclude that all the operations in the acquisition process are critical and potentially unrepeatable.

The investigative process starts from the acquired material and is aimed at analyzing the evidence and interpreting and presenting the

results. Each operation can therefore be repeated starting from the forensic copy.

A close collaboration is required between the skilled technician and the investigator who has a full and accurate grasp of scope of the investigation.

In the extraction and analysis phase, the digital evidence extracted from the source equipment is identified and evaluated. Specialized software is often used to discover digital data, as the volume of data that needs to be analyzed can be vast. Here we have a first point to discuss. Should tools used be validated? How can we really verify result if forensic software is not open source? [38].

Interpretation is the step where an investigator infers information from facts. The aim is to derive meaning from digital evidence, evaluating it in the context of circumstances. For example, a file being contained in a device is a fact. If the file was saved with a user-specified filename, it would be reasonable to infer that the user was deliberate in making that choice. The goal is to explain the facts detected over the course of the analysis.

In this phase there are circumstances that may make it necessary to go back to the initial step, where the data was identified. For example, if an analysis reveals that some of the data are missing from the system being analyzed but may be found elsewhere, then the entire procedure will have to be repeated on another device [39].

In our opinion it is particularly difficult at this stage to separate technical skills from investigative ones: both are important and need to be integrated.

Finally, the two final steps, reporting and presentation, are going to lead to the closing of the investigation.

---

[38] The issue on the usage of open-source software in digital forensics, especially in acquisition and analysis phases, is a well-known topic in the literature. In fact, if software whose source code is secret is used, a scholar has observed that «there seems to be a deficit of protection for the defence, since the latter, unable to check the correctness of the program's operation, may not be able to verify the activities carried out by investigators. Also, for this reason, exclusive use of open-source programs is desirable, with countless advantages for all procedural actors, including the possibility of verifying the activities carried out on the data even after years, given the easy availability of the software itself»: L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 2011, p. 4509. See also E. HUEBNER-S. ZANERO, *Open Source Software for Digital Forensics*, Springer, New York, 2010.

[39] Consider a scenario in which an email is found that brings into the conversation a third party who may in turn come under investigation, along with all the devices held by this person.

In particular, the reporting should contain all the documentation acquired or produced during analysis. It needs to contain scientific explanations in order to make possible to verify all the assumptions made during the investigation, moreover it must specify the tools and method used. The report should be written in a clear, concise, and unambiguous manner. The report is also the basis of the presentation, whose main purpose is to offer a live demonstration of the results obtained.

In the final verification phase, an independent expert or one of the other authorized parties must be able to inspect the activities carried out by the DEFR and the DES: all the operations they have gone through need to have been documented, so as to make it possible to determine whether all the appropriate methods, techniques, and scientific procedures have been used. One of the tools that has traditionally been used to reconstruct the way these technicians have worked in arriving at a given result – and so a tool that makes it possible to review the work done on the data, and to do so even at a distance of several years – is an open source software. But numerous competing proprietary software products have since come onto the market: we have reached a point where the key element in any verification lies in the ability to reproduce the same results by different means or methods. The OLAF Guidelines do not comment on this point, but generally a verification can make it necessary to backtrack all the way to the acquisition phase.

6. *The digital forensics lab: tools, facilities, and requirements*

It is no less important to digital investigations that *specialized labs* be set up where digital evidence can be managed. This includes the ability to create *virtual environments* which are remote from the places where investigations are conducted, and which also make it possible to automate certain phases in the forensic process of managing, storing, analyzing, and interpreting data. These labs can store large amounts of data, effect secure communications, carry out authentications on several levels, and check access based on one's role. And they are also equipped with forensic tools for managing cases, enable multiple virtual machines to share the same hardware. A centralized digital forensics laboratory provides investigators with the advanced tools they need for their work, making the best use of resources and skills, and bringing down the cost of forensic investigations.

First labs were created about a decade ago, but they came up against the limitations of technology and the challenges faced in getting the courts to admit evidence that had not been gathered in any of the traditional ways. But then came the surge in cybercrime. In response, an international legal framework was developed that could act as a support, and governments began to call for a more effective use of forensic science. It is against that background that many new initiatives followed and flourished, with the development of shared platforms and virtual labs in various sectors of forensic science [40], and with the adoption of methods that can be applied on a large scale.

Forensic investigations in real time can bring multiple advantages, and the uptake of this approach has the potential to make the criminal justice system much more effective. Consider live forensics, for example, where a power outage can cause the loss of volatile memory containing critical data, especially in cases involving encrypted devices (using encryption passwords), extensive memories, or the use of anti-forensics techniques [41].

However, the use of forensic tools of this kind also raises some issues: best practices require to continually test the hardware and software tools used in examinations, and most examiners unfortunately lack the skills necessary to validate them.

Even so, once these problems are overcome under a proper system of governance, the growth of cloud and virtual environments suggests that digital forensics labs will in the future be increasingly centralized and not constrained within geographic boundaries.

A digital forensics lab must have the following features: a surveillance system, to monitor the premises for unauthorized access and break-ins; access control; a fire-control system; reinforced windows, doors, and walls to prevent break-ins; a sufficient number power sockets, fuses, breakers, and current load; anti-static flooring; a radio-jamming system; a cooling system, because overheating can lead to loss of data and may damage hardware; off-site data storage backup, so that in the event of disaster, the offsite storage can be

[40] From 2012 to 2017, the European Forensic Genetics Network of Excellence (EUROFORGEN-NoE) built a virtual forensic genetics lab with partners from nine countries (scientists, scholars, law enforcement officials, and members of the judiciary) who collaborate in criminal investigations involving issues of privacy and the protection of minors.

[41] Anti-forensics is a set of techniques that can be used to conceal digital evidence and thus thwart the work of investigators trying to find it.

used to gain access to critical data; and archival long-term data storage. A digital forensics lab also needs some common facilities, like a reception area, one or more evidence-storage rooms, an evidence-processing area and laboratory, a personal space, and a briefing space[42]. Obviously, a digital forensics laboratory must be technologically equipped with several kinds of hardware and software for forensics acquisition and analysis, along with mobile kits for work outside the lab itself.

As said, OLAF has its own forensic laboratory. The laboratory is an isolated and protected space, the internal network is isolated from the Internet and Intranet. Access to the laboratory is limited only to specified people and after identification, and the entrance is under video surveillance.

OLAF has a lot of digital forensics hardware and software, and trained operators, so it does not need to rely on third parties for the performance of its activities of acquisition, analysis, and reporting. That is perfectly coherent with the international scientific recommendations, which insist on both the importance of the staff and the instruments.

The COVID-19 pandemic has further highlighted the importance of smart working. Even if most DESs are already equipped with laptops that they can bring into the field, the transition to smart working is not so easy. It is true that most of the analytical work can be done remotely, but digital forensics laboratories need policies and standard operating procedures to govern what DES can and cannot do from home. They include: ensuring employees harden their home networks, updating router firmware and changing Wi-Fi passwords regularly; having a virtual private network (VPN) available, in order to secure data in transit. Moreover, no original device must leave the lab space, but only forensic copies in encrypted devices, tracking everything and returning them; workstations must be encrypted and locked when DES is not working, to avoid access to sensitive data by people in the home environment. Another necessary requirement is the strong coordination among forensic experts and lab managers, who are in charge of ensuring the respect of the policies (for example, new purchases or replacements for broken technology).

---

[42] See the INTERPOL Global Guidelines for Digital Forensics Laboratories, available at *interpol.int/content/download/13501/file/INTERPOL_DFL_GlobalGuidelinesDigitalForensicsLaboratory.pdf*.

Anyway, some operations can only be performed in a lab, like identification and acquisition phases. So, to ensure that the lab work is being done without unnecessarily risking the examiners' safety, the team must identify the member who can go to the lab during a targeted time frame on a given day each week. That examiner must work from a list of needs. All laboratories should make these rules on their own.

7. *The big amount of data: technical requirements versus privacy*

Modern investigative activities are increasingly dependent on the interpretation of huge quantities of digital data of various kinds. This makes it very time-consuming to extract and analyze data, with great computing power, and moreover it makes the process extremely sensitive, owing to the risk that the confidentiality or secrecy of the information being analyzed may be compromised. This brings a dual aspect into the picture. The first one is tied to the need to ensure that digital investigations are effective and efficient, as well as that the necessary data is acquired in its entirety. The second one is instead tied to the right to dignity in what concerns one's digital life, a consideration that is moreover inseparable from the confidentiality or secrecy of all the information that coexists in virtual spaces. The issue therefore arises as to how to delimit the scope of an investigation, and in which phases, in the effort to find all the information that is relevant to the case at hand, all the while excluding all private and irrelevant data from the scope of the analysis and interpretation.

This issue is particularly relevant specifically in connection with the antifraud effort. As anticipated in Section 3.2, the OLAF Guidelines seem to veer away from the benchmark technical standards, at least in part, by taking a more considered approach. OLAF's general rule is that an investigation needs to proceed with a complete forensic acquisition of data, as the technical standards require, but that, if possible, the DES and the investigator need to have it in their discretion to display a preview of the data so as to assess whether to only acquire part of it. The 2013 *Guidelines on Investigation Procedures for OLAF Staff* a sort of general operating manual, also require at Article 15 that the digital forensic examination and analysis of the data collected in a digital forensic investigation be *limited to extracting data that is necessary and relevant to the same investigation* (§ 15.3). As explained *supra*, § 3.3, the DES has to extract and hand over to the investigator only the data that are pertinent to the

investigation. Indeed, in order to extract data from the forensics lab, the investigator must submit a written request to the DES specifying the exact object of the data search, meaning that the investigator cannot ask for a blanket acquisition of data, but must define a logical criterion in light of which to decide what to extract and what to leave out. The DES will produce in read-only format exclusively those files that meet the search criteria specified by the investigator: all other files will remain in the lab.

This last example, too, underscores the need to set out clear limits to the admissibility into evidence of forensic copies; if the entire collection enters the case file, the parties could consult it and gain access to data that are not pertinent to the legal proceedings. Note that in making a forensic copy, the aim is to make sure that the data being copied is not altered: it is not to produce the copy itself as the result of an investigation.

This is a critical point, and it means that the forensic copy is to be understood as a tool supporting the work of the digital forensic expert.

It is clear that when the parties are not involved in the fact-finding process, a forensic copy also becomes the probative element from which to start in carrying out that process. But how to proceed when the parties have the option of taking part in the process?

A forensic copy contains a huge quantity of data, and most of it will often bear no relevance to the technical investigation.

Take any case of any kind (child pornography, fake invoicing, intellectual property infringements): the data that are relevant to the fact in dispute, no matter what their quantity is, will only amount to a fraction of the data stored on the digital device being examined.

The figure below (n. 3) illustrates the entire process that runs from the acquisition of data to the analysis and selection of pertinent files.

Figure 3 – The process of identification of relevant files

Along with the relevant data, there will be a huge quantity of data that the parties concerned – the owner of the device, its user, or third parties whose data may be stored in it – would reasonably expect not to be captured, disclosed or taken into account: this includes projects, patents pending, family albums, and intimate messages, among other examples.

However, the need for confidentiality must be balanced against the need to preserve the integrity of the data for which a forensic copy is required.

In reality, the forensic copying of data is an operation that is instrumental to the subsequent data-analysis phase, in which it will be necessary to select pertinent data.

This brings into focus an interesting method by which to meet both of these two competing needs, and it rests on the idea of an impartial technician (a court-appointed or party-appointed expert) entrusted with reviewing all the data so as to select the pertinent data and leave out all data that is not pertinent.

The culling of such data can be done in an extremely granular way, looking at the files one by one, often with a great expenditure of resources (both time and money), or it can be done by applying objective selection criteria, which may also be used in combination. This can be done, for example, by searching for files having identical hashes or filtering a search by date, keyword, filetype, or interlocutor [43].

If these data-analysis activities are carried out adversarially, the parties involved who are bound by an oath of confidentiality would be in a position to assess the pertinence of the data that has been captured, requesting that only the data that are strictly necessary be introduced as evidence, and that all other data be "destroyed" [44].

---

[43] A variety of filtering tools are available. These include open-source tools like Autopsy, the search tools built into operating systems, and more advanced proprietary analytics tools like Xways, FTK, Nuix or Intella.

[44] This selection must take place in the presence of both parties, in a closed hearing, out of the public eye, otherwise it would lose its effectiveness. The immediate destruction of not relevant data to protect confidentiality may appear risky (errors or omissions would be impossible to remedy, and changes in the prosecution's line could be hard to face without the original set of data). However, it has nothing different from the excerpt of an intercepted conversation, or from the restitution of previously seized items (a car, a flat...). A compromise could be the maintenance of a sort of "safe storage of the forensic copy", under lock and key, to be able to access the entire collection in case it should be necessary.

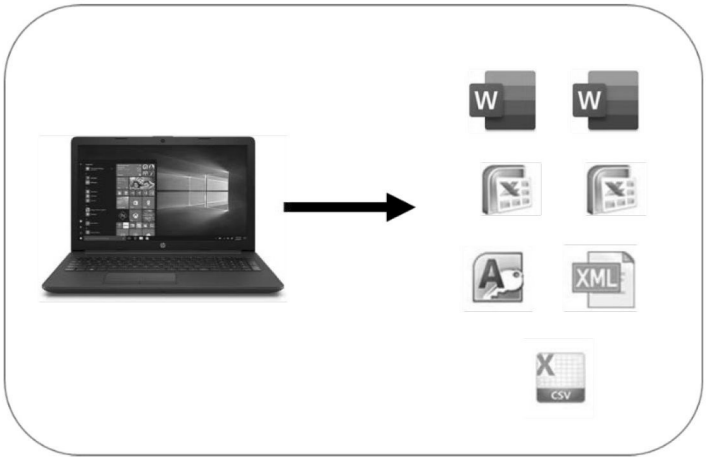

Figure 4 – Exemplification of the selection of data that is limited to what is relevant

The figure above (n. 4) illustrates the result of a selection process omitting all the intermediate passages, including the making of a forensic copy that would not be presented at trial because all concerned parties were able to contribute to the adversarial selection of the relevant files.

It is worth noting that, in Italy, this model is already in wide use in some kind of cases, for instance: in proceedings involving copyright infringement, where it would be unreasonable to grant access to the counterpart's industrial secrets. We are also beginning to see the first cases of this model being used in criminal proceedings in Italy in which a prosecutor, pursuant to Article 360 of the Code of Criminal Procedure [45], tasks an expert with performing a non-repeatable technical ascertainment, and is asked by the defence – as it is its right – to proceed with a special evidentiary hearing (*incidente probatorio*). At that point it will be up to the judge of the evidentiary hearing to appoint an impartial expert witness to task with analyzing the data, always respecting the fundamental tenets of an adversarial procedure. The forensic copy is thus only an intermediate working tool that gets destroyed once the data is selected as evidence, thereby requiring greater precision in describing the data that have survived the process of selection.

[45] In this case, the defence can only assist and express observations but has no right to veto respect the activity of the expert witness.

Under the proposed method, the prosecutor should perform a non-repeatable ascertainment (except if the "safe storage of the forensic copy" is implemented) enabling the counterpart to actively participate in the selection process. This choice clearly means that those findings need to be disclosed and that is why the selection is fundamental to protect the privacy.

It is furthermore evident that this way of selecting the evidence requires the investigating expert to have a proper appreciation of the criteria under which the proceedings are to be carried forward, which not infrequently places experts in a position where they have to make decisions about the parties' conflicting claims (with one party asserting that the data is relevant to the case, the other denying such a claim). Nor should it be discounted, finally, that the process of joint selection of the evidence can significantly delay the process, beyond what it would take for an independent analysis of the data, which can be verified and challenged at a later stage by re-examining the forensic copy.

8. *Conclusions: recommendation and perspective*

Taking account of the inherent features of digital evidence, we have used the methodological approach of digital forensics to outline a minimal set of activities for the proper handling of digital evidence within the framework of the technical and methodological standards that serve as a benchmark in the sector. We have further analyzed the roles and qualifications of the professional figures entrusted with digital investigations, identifying a skillset for the digital forensic expert. In our opinion it is particularly difficult to separate technical skills from investigative ones, indeed both are important and need to be integrated.

What emerges from the research is the pressing need to train and certify those to whom these activities are entrusted, and to invest in the infrastructure and research needed to support them. This includes building specialized labs for handling digital findings, and we described the characteristics these labs should have, even considering the experience of COVID-19 and the perspective of smart working, that need to be considered in the OLAF guidelines [46]. Furthermore, we suggest other additions in the next

[46] In the guidelines, only a physical isolated and protected laboratory is foreseen.

version of OLAF guidelines: for instance, they would be substantially improved by emphasizing the issue of the reproducibility of the analysis, which means that the results should be reached by different means or methods that those employed in the first place. The Guidelines could also be more helpful if they could guide the expert through the acquisition process, in particular, by establishing priorities. Moreover, they could be updated in order to respond to the technological progress, in particular reference to the cloud solutions (virtual machines, cloud storage...), which radically change the approach in the phases of identification, collection and acquisition. The Guidelines could also establish significant reliability thresholds by pay more attention to verifiable reports (both oral and written) that explain fully and clearly what was done and why, justifying the choice, especially when it comes to the information disclosed by service providers (included cloud service providers), since it is entirely up to the service provider to guarantee the quality of data collected and delivered to the authorities.

Finally, it was pointed out that the selection of data that may be relevant to the investigation – where the national legal system allows it – makes it necessary to take antifraud measures so as to properly address the typical problem of unsecured data stored on digital devices and virtual spaces. Considering the continuous increase of memories and the amount of data produced by citizens (also extraneous to the case), this is a proposal to safeguard personal data that are unrelated to the investigation. This is also an important requirement in Guidelines on Investigation Procedures for OLAF Staff at § 15.3. In this connection, we propose an alternative selection method by which to balance the competing desiderata calling for investigations at once complete and confidential. This highlights the need to achieve synergy between the different partiests and processes involved in an investigation: this is key to ensuring due process and to obtaining scientifically valid and highly reliable factual finding.

Sabine Gless-Thomas Wahl

THE HANDLING OF DIGITAL EVIDENCE IN GERMANY

OVERVIEW: 1. Digital Evidence in Germany – Virtually Unknown? – 2. National Legal Framework on Digital Investigations. – 2.1. Using Technology and Constitutional Limits: Clandestine Access to Data by Law Enforcement. – 2.2. Transfer of Rules from the Analogue to the Virtual. – 2.3. Delineating Open and Covert Investigative Requirements – Seizure of Emails as a Case Example. – 3. Ensuring Data Integrity – the Technical Side of Digital Evidence in Germany. – 3.1. Procedure of Digital Investigation – Involved Persons. – 3.2. Rules on "Digital Investigations". – 3.2.1. Guidelines. – 3.2.2. Best Practices. – 3.3. Practical Implications. – 4. Defense Rights. – 4.1. Right to Information. – 4.2. Right of Access to Files. – 4.2.1. Right to Access the File by Defense Counsel. – 4.2.2. Right to Access the File by the Defendant without Defense Counsel. – 4.3. Remedies against Investigative Measures in Relation to Digital Evidence. – 4.3.1. Covert Investigative Measures. – 4.3.2. Other Coercive Measures, e.g. Search and Seizures. – 5. Admissibility of Digital Evidence at Trial. – 5.1. Exclusion of Evidence Stipulated in the Law. – 5.1.1. Ban from Using Evidence Concerning the Core Area of Privacy for Interception Measures. – 5.1.2. Protection of Professional Secrets. – 5.1.3. Use of Digital Evidence in Other Proceedings. – 5.2. Exclusion of Evidence not Stipulated in the Law. – 6. Conclusions.

1. *Digital Evidence in Germany – Virtually Unknown?*

German law has a reputation of being sophisticated, principle-oriented and sharp. With regard to digital evidence, the situation looks quite different: Germany has neither a body of laws specifically governing the handling of digital forensic procedures nor does it have procedural rules for digital evidence [1]. Understanding of

[1] E. Basar, *Anforderungen an die digitale Beweissicherung im Strafprozessrecht und in internen Untersuchungen*, in *Festschrift für Jürgen Wessing zum 65.*

the terms "digital forensics" and "digital evidence is extremely wide, with proper definitions lacking. "Digital forensics" (frequently called "IT forensics" or "computer forensics") is considered a part of forensic science/criminalistics and is generally defined as detecting, securing and analyzing data that contains traces, which prove human behavior, by applying sound methodological processes [2]. "Digital evidence" is understood as all kind of personal and non-personal data, i.e. binary codes, that is stored digitally and includes evidence gathering related to IT systems [3]. It is considered a preferred means in order to obtain information to prove guilt or to exonerate a defendant. Courts use it to justify a verdict along with "classical forms" of evidence, such as witness testimonies or paper documents. A review of legal scholarship brings forth three observations that merit special mention at the very beginning of this chapter:

First, we lack a thorough debate outlining the need for specific rules governing digital forensics or digital/electronic evidence. In Germany, the current discourse focuses on possibilities to fit digitized information under the existing criminal procedural rules. Naturally, manifold problems arise as the German criminal procedure is tailored to the analogue world. Regarding digital forensics, courts or legal scholars engage less with the question of whether a new technology can be applied "lawfully" or whether it has to be "made lawful", but rather look for options to adjust new technologies under existing laws and rules based on general principles [4]. This pertains especially to the requirement of an IT forensic tool not infringing the (suspected/accused) person's core privacy – a "red line" for any state encroachments restricted by the Federal Constitutional Court and based directly on fundamental rights [5].

Second, it appears that IT forensic operations are currently so

---

Geburtstag, C.H. Beck, München, 2015, p. 639 points out that basic rules of criminal forensic are generally not regulated in the procedure laws.

[2] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, *Leitfaden IT-Forensik,* 2011, p. 8; D. HEINSON, *IT-Forensik*, Mohr-Siebeck, Tübingen, 2015, p. 1; A. GESCHONNEK, *Computer Forensik*, 6th edition, dpunkt.verlag, Heidelberg, 2014, p. 8.

[3] S.T. MÜLLER, *Internetermittlungen und der Umgang mit digitalen Beweismitteln im (Wirtschafts-)Strafverfahren*, in *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, 2020, p. 96.

[4] D. HEINSON, *IT-Forensik*, cit., p. 6, 10 f.

[5] Federal Constitutional Court (Bundesverfassungsgericht - BVerfG), Judgment of 20 April 2016 – 1 BvR 966/09, 1 BvR 1140/09, in *Neue Juristische Wochenschrift (NJW)*, 2016, p. 1781, mn. 123 with further references; B. VOGEL, *Country Report Germany (Sections I.-III.B.)*, in U. SIEBER-N. VON ZUR MÜHLEN (eds),

diverse that it would be a Herculean task to establish guidelines for all forms of digital evidence [6]. In addition, the rapid technology development as well as the use of different systems and interfaces by providers and producers of devices make the establishment of guidelines probably a Sisyphean task. It seems more useful to provide advice for the specific forms of IT forensic operations, such as reading out SIM cards, decoding, accessing cloud computing data, monitoring trojans, using spyware, etc. [7]. Nonetheless, we will see that a basic framework exists in Germany as soft regulation, which has developed at least certain standards of a forensic methodology to carry out digital investigations.

Third, legal scholars use the term digital evidence ("*digitale Beweismittel*") [8], while stressing, however, that the definition is extremely wide [9]. Due to the lack of statutory regulations, it generally remains unclear what exactly is the piece of evidence that must be handled properly through an unbroken chain of custody for it to be legally considered valid evidence in court: is it "data" as such or a specific data carrier or storage. With a strong affinity to the analogue world, data, data carriers and storage media are often dealt with by the courts like "papers", if it comes to investigations in the "digital world" [10].

Access to Telecommunication Data in Criminal Justice. A Comparative Analysis of European Legal Orders, Duncker & Humblot, Berlin, 2016, p. 514.

[6] H. WENZEL, *Rechtliche Grundlagen der IT-Forensik*, in *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, 2016, p. 85 ff.; D. KOCHHEIM, *Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik*, 2nd ed., C.H. Beck, München, 2018, mn. 1771 ff.; M. ROGGE, *Moderne mobile Forensik für Strafverfolgungsbehörden*, in *Der Kriminalist*, 2015, p. 29.

[7] M. ROGGE, *ibidem*; regarding "Internet of things" cf. M. HOCH, *Das Internet der Dinge – Alles vernetzt?!,* in *Kriminalistik,* 2019, p. 635; for considerations with IT issues when carrying out searches and seizures, see W. BÄR, *EDV-Beweissicherung*, in H-B. WABNITZ-T. JANOVSKY, *Handbuch des Wirtschafts- und Steuerstrafrechts,* 5th ed. C.H. Beck, München, 2020, Chapter 28, mn. 34 ff.

[8] E.g.: C. ROXIN-B. SCHÜNEMANN, *Strafverfahrensrecht*, 29th ed., C.H. Beck, München, 2017, § 24, mn. 2; C. MOMSEN, *ZumUmgang mit digitalen Beweismitteln im Strafprozes*, in C. FAHL-E. MÜLLER-H. SATZGER-S. SWOBODA (eds), *Festschrift für Werner Beulke zum 70. Geburtstag*, C.F. Müller, Heidelberg, 2015, p. 871 ff.

[9] S.T. MÜLLER, *Internetermittlungen*, cit., p. 96.

[10] L. BLECHSCHMITT, *Strafverfolgung im digitalen Zeitalter – Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren*, in *Mulitmedia und Recht (MMR)*, 2018, p. 363; M. BRUNS, *Kommentierung des § 110*, in *Karlsruher Kommentar zur Strafprozessordnung*, 8th ed., C.H. Beck, München, 2019, § 110, mn. 2; S. F. GERHOLD, *Kommentierung des § 94*, in J.-P. GRAF, *BeckOK StPO*, 36th ed., C.H. Beck, München, 2020, § 94, mn. 3, 4.

With its strong tradition in inquisitorial proceedings, providing a broad truth-seeking mandate, German authorities see few restrictions upon themselves when conducting digital investigations. The general regulations that govern investigations are considered "technologically neutral", thus the reasoning is that, in principle, digital investigation can take place wherever data is stored. Data obtainment is generally regarded as little regulated and data can be seized at will from computers, databases storing traffic data and any other data carrier, like CDs, hard drives, USB sticks, mobile phones or other tangible information storage mediums. Digital investigations are also carried out on new technological gadgets, such as smart speakers, smart watches or smart cars [11]. Evidence gathering, however, faces stricter requirements, if it infringes upon an individual's rights, in particular, privacy rights. Also, digital evidence can only be presented in criminal proceedings if it can be integrated into the existing regime of criminal procedure. German criminal procedure law has the rule of strict forms of proof or "*Strengbeweis*" [12]. This means that only four types of evidence are admissible for fact-finding (and sentencing): Witness evidence; Expert evidence; Documentary evidence; and Evidence by personal inspection.

Digital evidence is not a separate legal category of evidence [13]. As a consequence (to the *numerus clausus* of evidence), digital evidence must be presented in one (or various) of the four types of evidence [14]. This causes problems as it is widely observed that the provisions of the German criminal procedure are tailored to human witnesses or physical evidence of the analogue world [15].

This article will argue that, up to now, German law has not made a clear transition from the analogue to the digital world. This causes

---

[11] M. HOCH, *Das Internet der Dinge,* cit., p. 636. For the possibilities of law enforcement authorities to intercept or get data from intelligent virtual assistants or intelligent personal assistants, such as Alexa, Cortana, etc. see S. GLEß, *Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter*, in *Strafverteidiger,* 2018, p. 671; L. BLECHSCHMITT, *Strafverfolgung im digitalen Zeitalter,* cit., p. 361.

[12] M. BOHLANDER, *Principles of German Criminal Procedure*, Hart Publishing, Oxford, 2012, p. 144.

[13] C. ROXIN-B. SCHÜNEMANN, *Strafverfahrensrecht*, cit., § 24, mn. 2.

[14] Concerning the facts other than those mentioned, an open evidentiary proceeding (*Freibeweisverfahren*) applies.

[15] D. KOCHHEIM, *Cybercrime*, cit., mn. 1982 ff.; C. WARKEN, *Elektronische Beweismittel im Strafprozessrecht – eine Momentaufnahme über den deutschen Tellerrand hinaus, Teil 1*, in *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt),* 2017, p. 289 (291).

many problems. The following two sections focus on the gathering of evidence. In the first part (2), we will outline the legal framework that applies to digital evidence. In line with the general aim of the DEVICES project, we will focus here on investigative measures that are applied by law enforcement authorities (i.e. public prosecution services and police/revenue authorities as officials assisting it) to directly obtain electronic data in the pre-trial stage of (criminal) proceedings. Thus, measures that need the involvement of third parties, in particular, service providers who provide certain data on a user of the services, e.g. the obtainment of traffic and location data, are not focused on.

The second part (3) will focus on rather technical details of forensic IT operations and tackle the most eminent problem in relation to the use of data in criminal proceedings, i.e. its susceptibility to variability and manipulation [16]. We will outline how German procedural rules ensure a "chain of custody", so that data can be used as reliable evidence at trial. The last two sections will tackle specific overall issues in relation to digital evidence. We will first address defense rights in relation to digital evidence, whereby a focus is placed on the rights to be informed and to have access to the investigation files as well as on the possibilities to lodge remedies against the collection and/or use of evidence (4). Finally, we move on to the presentation of evidence and outline particularities in the use of digital evidence in a criminal proceeding, in particular, with regard to the possible application of exclusionary rules (5). In conclusion (6), we summarize the reasons why the legislation on digital evidence in Germany is widely underdeveloped and outline a possible way forward as regards digital evidence in German criminal proceedings.

2. *National Legal Framework on Digital Investigations*

As mentioned above, the German Criminal Procedure Code (*Strafprozessordnung – StPO*; hereinafter: GCPC) does not distinguish between digital investigation and search/seizure regarding

[16] Cf. U. Sieber, *Gutachten C zum 69. Deutschen Juristentag. Straftaten und Strafverfolgung im Internet*, C.H. Beck, München, 2012, C 68; S. Gless, *AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials*, 51 *Georgetown Journal of International Law*, 195 (2020), p. 222-5.

non-digital information. A traditional distinction in evidence gathering is made instead between secrecy vs. openness or: short-term vs. long-term interventions. Thus, it is the mode of intervention, or the *modus operandi*, which determines the specific legal requirements for an investigative operation. These may include searches ex post or "in real time". The search and seizure of devices and reading out of stored data or the seizure of stored communication data, such as emails, on the one hand, and the covert investigation techniques of source telecommunication surveillance and online (=remote) search, on the other, are seen as the main legal bases for "digital evidence" in German law [17]. These measures are briefly outlined as follows.

2.1. *Using Technology and Constitutional Limits: Clandestine Access to Data by Law Enforcement*

In recent years, the German legislator has gradually expanded the scope of investigatory techniques, allowing German law enforcement authorities to encroach further in private areas. For instance, a clandestine, "real time" access to technical devices by using spyware/malware is now possible. This clandestine access either works through the so-called source telecommunication surveillance (*Quellen-Telekommunikationsüberwachung*) or online searches (*Onlinedurchsuchungen*), also dubbed as "state Trojans". Source telecommunication surveillance has been introduced as a special form of telecommunications surveillance, allowing law enforcement agencies access to data "at the source", i.e. prior to encryption [18]. An "online search" [19] provides access to any "information technology system" used by the suspect without his or her knowledge in order to extract data. Online searches can be carried out over a long-term period to obtain any data stored on the device. It is this invasiveness that is the main difference to source telecommunication surveillance. Accordingly, the online searches must meet similar requirements to acoustic surveillance on private premises [20]. The latter is considered

---

[17] E. BASAR-M. HIÉRAMENTE, *Datenbeschlagnahme in Wirtschaftsstrafsachen und die Frage der Datenlöschung*, in *Neue Zeitschrift für Strafrecht (NStZ),* 2018, p. 681 (footnote 2); similar S.T. MÜLLER, *Internetermittlungen*, cit., p. 97 f.

[18] Sec. 100a Subsec. 1, sentences 2 and 3 GCPC.

[19] Sec. 100b GCPC, officially entitled: "Covert remote search of information technology systems".

[20] Sec. 100c GCPC.

one of the most invasive investigative measure in Germany entailing high thresholds due to constitutional concerns.

The legal requirements for both source telecommunications surveillance and online searches had been shaped by the case law of the German Federal Constitutional Court (*Bundesverfassungsgericht*, hereafter: FCC). The FCC has developed detailed principles that have been specifically elaborated upon with regard to digital data or, more specifically, the protection of the digital sphere. In this context, the FCC "developed" two fundamental rights based on constitutional rights, i.e. the right to information self-determination [21] and the right to the confidentiality and integrity of information technology systems [22]. The FCC eyes clandestine, long-term surveillance, but does not generally exclude it. It established the premise that the deeper the intrusiveness into the fundamental rights, the more precise and the more restrictive the legislation must be, i.e. by precisely defining predicate offences, the necessary degree of suspicion, and the manner of a measure's implementation [23]. Infringements of lower intensity, however, may be justified on the basis of statutory general clauses [24]. As a result, source telecommunication surveillance and

---

[21] Federal Constitutional Court (BVerfG), Judgment of 15 December 1983 - 1 BvR 209/83, in *Official Case Reports BVerfGE* 65, 1.

[22] Federal Constitutional Court (BVerfG), Judgement of 27 February 2008 - 1 BvR 370/07, 1 BvR 595/07, in *Official Case Reports BVerfGE* 120, 274, in *Neue Juristische Wochenschrift (NJW)*, 2008, p. 822 (Ger.). This right was developed when the FCC examined the constitutionality of the power of the secret service of North Rhine-Westphalia to surreptitiously monitor and investigate the Internet, including information technology systems. This power for online searches by intelligence services was transferred to the prosecution of crimes. For an analysis of the FCC's judgment in English, see W. ABEL-B. SCHAFER, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822*, in *SCRIPTed,* vol. 6 (2009), p. 106.

[23] See Federal High Court of Justice (BGH), Judgement of 14 May 1991 – 1 StR 699/90, in *Neue Juristische Wochenschrift (NJW)*, 1991, 2651 (Ger.); G. PFEIFFER, *Strafprozessordnung*, 5th ed., C.H. Beck, München, 2005, Section 161, para. 1. For the fundamental rights challenges in relation to the examination and seizure of computer systems and communication, mobile and smart phones, and Skype, the seizure and reading out of emails and chat room messages, SIM cards, see H. WENZEL, *IT-Forensik*, cit., p. 88 ff.

[24] While upholding the rule of law, *i.e.* any infringement of individual rights needs a legal basis, the FCC nevertheless agrees that certain investigative measures are not invasive and thus may be based on a general clause (Section 161 GCPC for the public prosecutor and Section 163 GCPC for the police). Thus, the competent law enforcement bodies are entitled to request information from authorities and to

online searches are subject to restrictions as regards personal and material scope. They can only be applied when investigating serious offences [25] and proportionality is always an issue (the offence must be one of particular gravity in the given case and other means of establishing the facts or determining the accused's whereabouts must be significantly more difficult or offer no prospect of success). In addition, the law includes several "securing mechanisms", including requirements for the surveillance software, the scope of admissible alterations to the information technology system, their rescissions, protection of data against unauthorized use and documentation obligations [26]. These specific provisions for source telecommunication surveillance and online searches strive to ensure data integrity and conservation of the evidentiary value of the data [27]. Surprisingly to scholars, these new forms of clandestine surveillance have not been widely used in practice to date [28].

2.2. *Transfer of Rules from the Analogue to the Virtual*

In practice, there are often no specific tools, but public prosecutors routinely focus on specific investigatory measures, e.g. acquisition of traffic and subscriber data, seizure of emails or server monitoring (the latter by using the covert investigation method of telecommunication surveillance as set out in Sections 100a et seq.

---

conduct investigations based on the so-called "*Ermittlungsgeneralklausel*" (Federal Constitutional Court (BVerfG), Judgement of 10 March 2009 – 2 BvR 1372, 1745/07, in *Neue Juristische Wochenschrift (NJW)*, 2009, 1405 (Ger.)). This includes, for example, data collections in social networks or the public prosecutor's request from banking institutions for information about certain credit card payments on a hit-no hit basis (W. BÄR, *EDV-Beweissicherung*, cit., Chapter 28, mn. 6). The general investigative clause is, however, only applicable provided there are no other statutory provisions specifically regulating the law enforcement powers. More invasive encroachments into fundamental rights need specific, more precise legislation, such as searches and seizures or interceptions of telecommunications. If the formal and substantive legal prerequisites of these measures are not met, the measure is not rendered lawful by resorting to the general clause.

[25] The law (GCPC) defines these offences in catalogues, referring to offences stipulated in the German Criminal Code or other codes/acts, *e.g.* the Fiscal Code.

[26] Sec. 100a, Subsec. 5 and 6; Sec. 100b, Subsec. 4 GCPC.

[27] E. BASAR-M. HIÉRAMENTE, *Datenbeschlagnahme*, cit., p. 682; C. WARKEN, *Elektronische Beweismittel im Strafprozessrecht*, cit., p. 335.

[28] The main reasons are difficulties in the technical realization of the spyware and in keeping pace with the technological developments. For the legal and practical hurdles de lege lata, see also B. DERIN-S.J. GOLLA, *Der Staat als Manipulant und Saboteur der IT-Sicherheit*, in *Neue Juristische Wochenschrift (NJW)*, 2019, p. 1111.

GCPC) [29]. As was confirmed in the interviews [30], the seizure of a computer or other devices and the subsequent read-out of the data remains the most relevant operation in daily practice (even if investigations into tax crimes are conducted [31]). As described above, the hurdles for covert investigations are rather high due to their invasiveness upon individuals' fundamental rights enshrined in the German constitution. Therefore, investigators must resort to measures applied openly. In general, the hurdles for open measures are less stringent than those for covert ones. This is especially the case for the "seizure of data" stored on a device in the possession of a defendant. Such seizures are based on Section 94 GCPC. The prevailing opinion is that it not only allows the seizure of tangible objects, such as a computer or smartphone, but also "intangible" objects, such as the data stored on the devices [32]. It is not always necessary to seize the device, but the seizure can also be carried out by producing data copies and submitting them to specialized crime units of law enforcement for digital analysis. Considering the way such data is "secured" and collected, and the amount of data that may be potentially involved, it is – in nearly all cases in this context – very much disputed whether the measures can still be based on the provisions that were developed for tangible/physical objects or whether they must be subjected to the legal basis for covert investigations, in particular, those on telecommunication surveillance. This aspect is particularly important since the prerequisites for the measures considerably differ.

Regarding the search and seizure of stored communication data, *Köppen* summarizes the dilemma well: «Thus far, the system of rules on search and seizure has hardly been adapted to the requirements of the digital age. Due to a lack of alternatives, the existing procedural instruments must be used. Regarding the search for electronic (communication) data, these are the rules on the search of private premises, persons, and objects for the purpose of discovering evidence, Sections 102 et seqq. StPO [GCPC]. But the basis upon which this evidence may be permanently secured or seized has not been completely resolved for every type of case. The main provisions worth considering in this respect include, on the one hand, the general rules on seizure in Sections 94 et seqq. StPO,

[29] D. Kochheim, *Cybercrime,* cit., mn. 1809.
[30] Interview with Klaus Hoffmann.
[31] H. Wenzel, *IT-Forensik,* cit., p. 85.
[32] L. Blechschmitt, *Strafverfolgung im digitalen Zeitalter,* cit., p. 364.

which are tailored to apply to tangible objects, as well as the corresponding special provisions on the seizure of postal items pursuant to Sections 99 et seq. StPO, and, on the other hand, the regulations authorising the surveillance of intangible telecommunication in Sections 100a et seq. StPO»[33].

2.3. *Delineating Open and Covert Investigative Requirements – Seizure of Emails as a Case Example*

In practice, the access to email content is highly relevant[34]. Yet, surprisingly, pivotal legal issues regarding this measure, are not regulated by legislation. Thus, we find highly divergent interpretations of relevant general rules in case law and literature. Courts concur that, as a rule, the provisions for the seizure of physical objects apply also for the seizure of data on a storage medium in an analogous way (Sections 94 et seq. GCPC). Seizures on the basis of Sections 94 et seq. GCPC require (only) that «objects may be of importance as evidence for the investigation» but are not surrendered voluntarily (Section 94 Subsection 1 and 2 GCPC). The law does not require a certain degree of suspicion: It suffices if it is possible that, based on experience, an offence may have been committed[35]. Seizures are restricted by the provisions prohibiting the seizure of certain objects (e.g. «written correspondence» between the accused and the persons who may refuse to testify) and the proportionality principle. From a formal point of view, seizure requires, as a rule, an order by the court (Section 98 Subsection 1 GCPC).

While it is settled case law that emails or messages still to be transmitted or already stored on a computer or mobile phone can be seized pursuant to Sections 94 et seqq. GCPC, with no intrusion of the fundamental right to secrecy of telecommunications[36], it is

---

[33] P. KÖPPEN, *Country Report Germany (Sections III.C.-IV.)*, in U. SIEBER-N. VON ZUR MÜHLEN (eds), *Access to Telecommunication Data in Criminal Justice. A Comparative Analysis of European Legal Orders*, Duncker & Humblot, Berlin, 2016, p. 552.

[34] M. GERCKE-P. BRUNST, *Praxishandbuch Internetstrafrecht*, W. Kohlhammer, Stuttgart 2009, mn. 808; D. KOCHHEIM, *Cybercrime*, cit., mn. 2022.

[35] *Anfangsverdacht*. See, in general, M. BOHLANDER, *German Criminal Procedure*, cit., p. 70; for seizure: L. MEYER-GOßNER-B. SCHMITT, *Strafprozessordnung*, 63th ed., C.H. Beck, München, 2020, § 94, mn. 8.

[36] Federal Constitutional Court (BVerfG), Judgement of 2 March 2006 – 2 BvR

fiercely debated according to which provision an ongoing email exchange could be monitored. The proposed option for surveillance of ongoing telecommunication is Section 100a GCPC with its stricter requirements [37].

The debate in this context erupted around authorities (openly) seeking access to emails stored with the recipient's provider. The Federal Court of Justice (*Bundesgerichtshof*) argued that the measure is equivalent to the provision allowing the seizure of «postal items» (Section 99 in connection with Section 94 GCPC), so that access to online mailboxes need not take the hurdles of Section 100a [38]. This approach was backed by the FCC. Interestingly, the FCC argued that temporarily or permanently stored emails with the provider may indeed fall under the protection of the secrecy of telecommunications (Art. 10 of the Basic Law), but the current provisions on the seizure of tangible post items in Sections 94 and 99 GCPC suffice to justify the encroachment. However, law enforcement authorities must respect the principle of proportionality by balancing the interests on a case-by-case basis [39]. This was surprising since academic literature assumed that encroachments on the fundamental right to the secrecy of telecommunications can only be based on Sections 100a et seq. GCPC. Academics further argue that the intermediate storage at the recipient's provider server is an immanent process of the entire communication, so it makes no sense to treat this phase differently to an intrusion into ongoing telecommunications. It is also feared that the superior courts' case law lowers the level of protection for the person concerned [40].

Not decided yet by higher courts is the situation when law enforcement authorities seek data access without the knowledge of the person concerned – possibly for an extended duration – by

---

2099/04, in *Neue Juristische Wochenschrift (NJW)*, 2006, 976 (978 ff..) (Ger.). However, if the access to emails is made externally via online search, the prerequisites of Sec. 100b must be respected (cf. W. BEULKE-S. SWOBODA, *Strafprozessrecht*, 15th ed., C.F. Müller, Heidelberg, 2020, mn. 392).

[37] This is assumed in the following phases: first, after having been dispatched by the sender and prior to arriving at the sender's provider; second, after having been dispatched by the sender's provider and prior to arriving at the recipient's provider; and third, during retrieval by the recipient. See P. KÖPPEN, *Country Report Germany*, cit., p. 555; W. BEULKE-S. SWOBODA, *ibidem*.

[38] Federal Court of Justice (BGH), Decision of 31 March 2009 – 1 StR 76/09, in *Neue Zeitschrift für Strafrecht (NStZ)*, 2009, 397 (Ger.).

[39] Federal Constitutional Court (BVerfG), Judgement of 16 June 2009 – 2 BvR 902/06, in *Neue Juristische Wochenschrift (NJW)*, 2009, 2431 (Ger.).

[40] Cf. W. BEULKE-S. SWOBODA, *Strafprozessrecht*, cit., mn. 392.

performing the interception at third parties (e.g. Facebook; cloud provider) to which the person entrusted the further transmission or non-local storage of her messages. Here, there is even disagreement by lower courts whether such measures can be based on the analogous application of seizure of postal items (Section 99) or whether here – because covert and potentially long-term – Section 100a on the surveillance of telecommunications is the (only) correct legal basis [41].

The example demonstrates that the German legal setting frequently triggers a debate as to which legal basis actually allows for data to be accessed in a specific situation for an investigative operation. Courts often favor allocating an invasive measure to a legal basis allowing an isolated/one-off intervention (with lower standards) instead of the more restrictive legal bases on covert investigations, such as surveillance of telecommunications. This allocation has broad consequences for prerequisites to be met [42], e.g. isolated/open investigative measures are, in principle, not restricted to certain criminal offences in contrast to the covert investigative measures governed by Section 100a et seq. GCPC (see above). Different rules between the open measure of seizure and covert investigative measures of telecommunication surveillance also exist, for instance, if it comes to the legal question of whether the measure can be ordered by the public prosecutor or even police officer in exigent circumstances (*Gefahr im Verzug*) without a previous court order.

3. *Ensuring Data Integrity – the Technical Side of Digital Evidence in Germany*

The basic difference between covert investigative and open investigative measures continues if we tackle the issue on the way digital investigations should be carried out and how the integrity of data is protected. Regarding covert investigative measures, Sec. 101

---

[41] Cf. P. KÖPPEN, *Country Report Germany*, cit., p. 557 with further references; L. MEYER-GOßNER-B. SCHMITT, *Strafprozessordnung*, cit., § 100a, mn. 6d.

[42] Another important issue of the allocation is that legal bases on covert investigations are considered *lex specialis*, thus open measures are actually excluded: cf. S. GLESS, *Wenn das Haus mithört: Beweisverbote im digitalen Zeitalter, in Strafverteidiger*, 10 (2018), p. 671-678. Instructive on the German approach, P. KÖPPEN, *Country Report Germany*, cit., p. 552.

GCPC sets out some procedural rules for undercover measures. These include that information acquired by covert measures must be labeled accordingly, in order to ensure – among other things – that the data will be deleted in time. Following transfer of the data to another agency, the labeling is to be maintained by such agency. As mentioned above, the legislator furthermore acknowledges problems in relation to the integrity of acquired data in information technology systems and included specific regulations in the legal bases for source telecommunication surveillance and online searches (Section 100a Subsections 5 and 6, Section 100b Subsection 4 GCPC). Specific legal rules for open investigative measures targeting data, such as the seizure of mobile devices, do not exist. However, it is common practice that the police officer follows routine procedures for seizure (of tangible objects). Nonetheless, Germany does not provide for legal rules as to how a data analysis or a "read out" of data on a device must be carried out [43].

In the following section, we will first give a general idea of how digital investigations are carried out, in particular, which persons are involved in a digital investigation within the criminal process. We will then guide the reader through the essential guidelines for digital forensics that apply as a type of soft regulation as well as other best practices. Third, we will examine the practical implications of data analyses carried out in the criminal process.

3.1. *Procedure of Digital Investigation – Involved Persons*

Depending on the particularities of a case, different persons within a police unit may be entrusted with digital investigations. Considering the type and seriousness of the offence, the public prosecutor may decide with police officers whether and how a digital investigation is carried out. If digital evidence is important for the case and special analytical expertise is necessary, a special unit within the criminal police (at the local/municipal level) may carry out technical operations and analysis.

If the special unit is involved, the procedure is regularly as follows:

1) A device/storage medium is seized by the local police officers;
2) One police officer is competent to conduct the investigations (can,

[43] L. Blechschmitt, *Strafverfolgung im digitalen Zeitalter*, cit., p. 364.

but does not need to be the same person seizing the device on the spot);

3) The competent police officer hands over the device to the special unit within the criminal police for technical analysis. These persons are IT forensic specialists.
4) The IT forensic specialist carries out the analysis and produces a technical report.
5) The competent police officer analyses the technical report and produces the content information needed for the prosecutor, i.e. he/she drafts a report in which the evidence is presented.
6) The public prosecutor assesses the police report. He particularly examines whether the content report and the presented data analysis is conclusive and comprehensive.

Hence, the police officer who is present at the "acquisition" phase (regularly a seizure of an object/of data) is usually different from the one who does a "technical analysis". The specialists at the special units are not handling the case, i.e. they do not make conclusions on the analyzed data. Their work is more or less limited to "data preparation", i.e. the technical part of a digital forensic analysis. Which data is to be prepared depends on what the prosecutor/police officer handling the case needs. In individual cases, the IT forensic specialists may also be present "on the spot" and carry out the necessary securing measures.

In sum, the involvement of the IT forensic specialists at the unit within the criminal police has to be decided in a pragmatic way and is a question of capacities and human resources. If technical analyses must be carried out by the unit, the investigations process is prolonged. In cases of less serious or "simple" crime, it may also be the police officer handling a case who does a "digital investigation", e.g. by reading chat communications, emails, etc. This is then, more or less, an inspection without technical specificities. Digital investigations have become a mass phenomenon; therefore, the public prosecution service has to filter out the cases which have to be submitted to the forensic specialists. Carrying out digital investigations is, therefore, less a legal problem and more a practical one.

IT forensic analyses may also be made at the Federal Criminal Police Office (*Bundeskriminalamt* (*BKA*)) or State Criminal Police Offices (*Landeskriminalämter* (*LKAs*)). BKA and LKA also employ IT forensic experts carrying out "digital investigations". They may have more technical possibilities as well as enhanced equipment in comparison with local criminal police units. In individual cases, the

BKA/LKA may also carry out an IT forensic analysis if it cannot be carried out effectively at the level of the local criminal police, thus having a support function.

Depending on the individual case and practice, experts outside the law enforcement bodies may be involved. It may happen that the public prosecutor, the trial court or the defense counsel mandate an external expert (e.g. a private digital forensic laboratory) to carry out digital investigations [44]. In the pre-trial stage, an expert (Sachverständiger) should only be involved if his expertise is indispensable to clear up the facts of the case [45]. The person may then either replace the IT forensic specialist at the law enforcement body or be involved in an additional capacity, i.e. in order to provide a "second expert opinion". Before the public prosecutor appoints an expert, he must give the defense counsel the occasion to make a statement, unless the prosecutor fears that this would endanger the purposes of the investigation or lead to a delay of proceedings [46].

If an expert is appointed by the court or during the investigation stage by the public prosecutor, the special provisions on expert evidence in the GCPC apply [47]. If the police officer who carried out an IT forensic analysis is to be heard at trial, she has the status of

---

[44] A further delineation must be drawn between an "expert" and an "investigator". The complete "outsourcing" of digital investigations, including the search for, sifting, and concluding analysis of data, to private entities would be inadmissible. This would be counter to the general clause empowering the state authorities to make investigations in Section 161 Subsection 1 GCPC (see also H. WENZEL, *IT-Forensik*, cit., p. 86 who also points out that in this case the evidence obtained would be fully inadmissible in trial). Likewise, a transfer of the investigations to other public bodies (e.g. the Federal Office for Information Security) which are not auxiliary officials of the prosecution office as defined by law (cf. Section 1, question 1) would not be possible.

[45] Nr. 69 RiStBV.

[46] Nr. 70 RiStBV.

[47] Sections 72 et seq. (Section 161a Subsection 1 GCPC). The expert privately retained by the defence counsel/defendant are not considered "experts" in the strict sense of the GCPC (Federal Court of Justice (BGH), Judgement of 24 July 1997 – 1 StR 214/97, in *Official Case Reports BGHSt* 43, 171 (Ger.)). Privately-retained experts do not have less evidentiary value per se. The distinction is rather a matter of who bears the costs of a "privately retained expert". See M. BOHLANDER, *German Criminal Procedure*, cit., p. 153 who points out that the advantage for the defence is that it has the right to have the report of its own private expert heard rather than that of a court-appointed expert, and is thus not restricted to a mere motion to appoint expert evidence.

"witness because of expert knowledge" (*sachverständiger Zeuge*), meaning the provisions concerning witness evidence apply [48].

3.2. *Rules on "Digital Investigations"*

3.2.1. *Guidelines*

There are no uniform standards for law enforcement on how to manage and handle digital investigations. The landscape is rather heterogeneous.

As regards the application of the forensic methodologies, the main reference work for both digital forensic experts within the criminal police and defense lawyers, who might challenge digital evidence, is the guidelines on "IT forensics" from the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik - BSI*) issued in 2011 [49]. The guidelines can be considered as a set of soft regulations, which have in fact been mainly addressed to system operators, i.e. the private economy, to cope with IT incidents (e.g. hacked company IT systems, lost data due to hardware or software problems, etc.), but it is stressed that the guidelines can also be used by law enforcement authorities [50]. They are designed both as a basic guide, which allows a deeper understanding of the matter, and a reference work for the solution of practical problems. IT forensics is defined as a strictly methodological data analysis on data mediums or computer networks, in order to investigate incidents, including possibilities of strategic preparation. The aim is to present a practice-orientated model for IT forensics through which the addressees can deduct recommendations and an action plan. The guidelines describe how information can be secured as evidence and data prepared. The described technique is widely independent from concrete forensic

---

[48] See Section 85 GCPC: The provisions concerning evidence by witnesses shall apply if experienced persons have to be examined to prove past facts or conditions, the observation of which required special professional knowledge. See also M. BOHLANDER, *German Criminal Procedure*, cit., p. 154, who points out that the literal translation of "expert witness" is misleading in view of the use of the term in the common law context.

[49] Leitfaden "IT-Forensik", Version 1.0.1 (März 2011), available (only) in German at: *bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2*.

[50] BSI Leitfaden "IT-Forensik", cit., p. 9.

software programs. The paper does not guide the analysts through the available forensic tools in detail. Instead, the focus is on a comprehensive and appropriate development of a methodology, which is why the guidelines – nine years after their issuance – can still be considered "up-to-date". As far as it is important for digital investigations by law enforcement, the BSI guidelines structure the investigation process into five parts: (1) operational preparation; (2) data collection; (3) examination; (4) data analysis; and (5) documentation [51]. These phases may differ from other international standards. The guidelines provide for a number of individual processes within the various stages, highlight the importance of the chain of custody [52] (stressing that integrity and authenticity of the acquired data and the applied technique must be guaranteed), and emphasize the documentation of all stages of the entire examination (who has done what, when and with which result?).

It has been established in interviews [53] that beside the BSI guidelines the various State Criminal Police Offices (*Landeskriminalämter (LKAs)*) follow standards based on guidelines adopted by the respective authorities themselves [54]. The State Criminal Police Office of Lower Saxony, for instance, established its own working and procedural instructions that are applied in everyday work. It was stressed that a focus lies on how the "chain of evidence" is ensured. In general, the common procedures for the inspection of seized objects also apply to data. Strict rules on how exhibits are managed are applied. This means, in particular, a precise documentation and application of the dual control principle.

3.2.2. *Best Practices*

An important role is conferred to best practices, which are partly also identified in the BSI guidelines. By now, certain practices have developed for specific investigative measures, in particular, the seizure of data and the access to data stored "in networks".

In case of seizure, law enforcement authorities can choose whether they seize the device or generate data copies on the spot [55]. Which

[51] BSI Leitfaden "IT Forensik", cit., p. 24.
[52] BSI Leitfaden "IT-Forensik", cit., p. 23, 90.
[53] Interviews with Klaus Hoffmann and Mathias Mertens.
[54] These guidelines are not publicly available.
[55] The underlying provision is Section 110 GCPC, which plays an important role

approach they choose will depend on several aspects. If the medium is a mobile device (e.g. mobile phone, USB stick, external hard drive, tablet, laptop), the entire device is regularly seized. In practice, authorities seek a forensic duplication of relevant data. This procedure ensures that a forensic investigation can be repeated several times without changing the initial data set. In addition, this method has the advantage that the data storage medium can be quickly returned to the owner, and thus the principle of proportionality is complied with [56]. In order to guarantee the function of the duplication, investigators should take into account [57]:

• IT forensic investigations require that data collection can be reconstructed;

• The duplication must be an exact/precise image of the original;

• The image of the original is proved by the hash value;

• The original set of data at the time of seizure must be documented by appropriate measures so that the evidentiary value of the investigation is not compromised at a later stage;

• Before any selection of data, the original set of data should be saved as backup;

• In practice, law enforcement authorities have a "working version" of the data to which any competent investigator has access, and the backup which remains at the IT expert.

It was confirmed in the interviews [58] that the exact duplication ("mirroring") of data and subsequent work with the data copy is the essential element in digital investigations [59]. The original data set remains "conserved". Furthermore, a detailed documentation and recording of the different steps carried out by the law enforcement

---

in the collection of "digital evidence". Initially developed in the framework of classical searches in the analogue world, it authorises the public prosecutor office and assisting officials (e.g. police officers and, in tax cases, customs investigation offices and tax investigators) to examine «documents» belonging to the person affected by the search. The term «documents» is used in a broad sense, including all written content, regardless of its physical form, thus including electronic data. If a storage medium is found in a search, the investigators are entitled to provisionally sift and secure data, in order to make a final seizure decision about data obtainment. The method of examination of the data storage medium pursuant to Section 110 GCPC is a form to choose the least invasive measure on the person concerned, so that the proportionality principle can be maintained.

[56] E. BASAR-M. HIÉRAMENTE, *Datenbeschlagnahme*, cit., p. 682.

[57] E. BASAR-M. HIÉRAMENTE, *ibidem*, with further references.

[58] Interviews with Klaus Hoffmann and Mathias Mertens.

[59] See also E. BASAR, *Anforderungen an die digitale Beweissicherung*, in *FS-Wessing*, cit., p. 642 who highlights that ensuring authenticity and integrity of the original data set is most important for forensic investigations from the outset.

authorities both in relation to the collection of the data and the subsequent analysis is very important.

In the area of live forensic measures, investigators regularly acquire a wide range of data as set out in directories. Securing this data *lege artis* mostly entails that so-called containers (data packages) are generated. These containers are handled similarly to forensic duplications, i.e. the IT expert does not touch or work with the generated container but stores it. The competent investigator receives extracted data from the container with which he/she is carrying out further processes [60].

3.3. *Practical Implications*

According to the interviews conducted [61] and the case law available, the (soundness of the) chain of digital evidence and the use of forensic methods for data analyses are usually not challenged in German proceedings [62]. The reasons remain unclear. If the aforementioned routine standards are maintained, there is usually no space for the defendant and her defense lawyer to attack the presented analysis and its results. These standards concern, in particular, the carrying out of analytical work on copies, whereby the original data set is "stored/conserved", managing data like exhibits (e.g. by documenting each access to the object after having secured it, recording any event in relation to the data object, and applying dual control) and documentation of history and results of the analysis, so that each procedural step can be followed at a later stage. One should also bear in mind that the guidelines – in particular, the BSI guidelines as the main reference work document and thus the basis for possible challenges by the defense [63] – are extremely complex and hardly understandable for a defense lawyer. Thus, defense lawyers usually lack the expertise to dive into the special technical details of

[60] E. Basar-M. Hiéramente, *Datenbeschlagnahme*, cit., 683.

[61] Interviews with Klaus Hoffmann and Mathias Mertens.

[62] More conflicts can be expected if it comes to data gained following the use of spyware in the framework of the controversial new covert investigative methods of online search and source telecommunication surveillance (see above). However, in these fields practical experience is currently lacking and no case law has been established yet.

[63] See above 3.2.1.

digital investigations [64]. In other cases, objecting to the results of digital analyses may be counter to the defense strategy: although the defense council may apply at the court for appointment of an external expert, involving experts is time consuming and expensive. If the defendant is convicted, he also bears the costs for the (potential) expert opinion. Another reason relates to the German law on exclusion of evidence and the "probability of success" of a challenge [65]: if the chain of evidence is "defective" there is no automated exclusionary rule; the evidence is subject to the principles of the free evaluation of evidence and unsound digital evidence might require other corroborating evidence.

4. *Defense Rights*

This part explains the most relevant defense rights, i.e. the right to receive adequate information about the rights throughout "digital investigations", the right to get insights into the reports filed during a digital investigation (see supra 3.2.) and the rights to lodge remedies if the defendant feels his/her rights have been violated.

4.1. *Right to Information*

Regarding the reception of information, we can make a similar observation to that made at the beginning of the previous two sections: German criminal procedure law includes precise regulations on notification obligations in the case of covert measures in the area of interception, whereas the norms seem incomprehensive if it comes to the application of classical open investigative measures like search and seizure to collect "digital evidence". Section 101 GCPC stipulates the persons who must be notified for each of the clandestine investigative measure. In the case of source telecommunication surveillance, for instance, the «participants in the telecommunication under surveillance» must be notified. In the case of online searches, notifications must be performed vis-à-vis the «targeted person» and «other persons significantly affected thereby».

[64] See also S.T. MÜLLER, *Internetermittlungen*, cit., p. 101.
[65] On the use of evidence, see more details below 5.

In addition, grounds dispensing with notifications as well as deferring them are stipulated.

In case of open investigations, in particular, when searches pursuant to Sections 102 et seq. or seizures pursuant to Sections 94 et seq. GCPC are conducted, the general rules apply that are specifically drafted for search and seizure of "papers": the persons affected by the measure have, for instance, the right to be heard [66]. According to case law, this right entitles all «whose (own) rights are infringed directly by the court order» [67]. Thus, beyond the formal parties to the proceedings, e.g. the defendant, all persons «substantially affected by the judicial decision» [68] can make a statement, and the statement must be acknowledged and taken into consideration [69]. In the specific cases of search and seizure, the person concerned must be given notice of the judicial order(s), including the reasons given for the respective decision (Section 34 GCPC). This must happen no later than the commencement of the measure. According to Section 33 Subsection 4 GCPC, a prior hearing regarding a seizure can be dispensed with if it would endanger the purpose of such an order.

The issue of whether, or rather how long, law enforcement authorities can defer the notice prior to a seizure is subject to controversial debate, as is non-disclosure of the justification to use this measure, if this would endanger the purpose of the investigation. In recent decisions, the Federal Court of Justice (*Bundesgerichtshof*) stated that the formerly common practice of non-disclosure is unlawful because the seizure is an open measure and Section 101 GCPC (see supra) cannot be applied in an analogous way [70]. However, even if the obligation to give notice to the persons affected is violated, this does not trigger exclusionary rules [71].

The lack of adequate notification obligations on authorities

---

[66] This right is stipulated in a general way in Art. 103 para. 1 of the Basic Law (the German constitution) and for criminal procedures at statutory level in Section 33 Subsection 3 and 35 GCPC.

[67] Federal Constitutional Court (BVerfG), Decision of 14 April 1988 – 1 BvR 544/86, in *Neue Juristische Wochenschrift (NJW)*, 1988, 1963 (Ger.).

[68] BVerfG, *ibidem*.

[69] P. Köppen, *Country Report Germany*, cit., p. 560 with further references.

[70] Federal Court of Justice (BGH), Decision of 4 August 2015 – 3 StR 162/15, in *Neue Zeitschrift für Strafrecht (NStZ)*, 2015, 704 (Ger.) expressly as regards seizure of data on the mail server of a provider.

[71] S. F. Gerhold, *Kommentierung des § 98*, in J-P Graf, *BeckOK StPO*, 36th ed., cit., § 98, mn. 11.

collecting digital evidence has been criticized for a long time. Scholars argue that open investigative measures – such as the seizure of emails – are ultimately more similar to covert investigative measures, such as the interception of telecommunications, without comparable procedural guarantees [72].

4.2. *Right of Access to Files*

Overall, individual rights in relation to the process and documentation of a "digital investigation" are not regulated adequately. In fact, this issue is considered a matter for general rules, in particular with regard to access to the file in a criminal case. Regarding the scope of the latter right, German law distinguishes, first between a defendant represented by a defense counsel and a defendant with no defense counsel (see Section 147 GCPC). Second, the law differentiates between the right to inspect the file and the right to inspect «officially impounded pieces of evidence» [73]. The latter are sometimes briefly named "exhibits" in explanations of German criminal procedure [74]. An essential question in regard to the mode of inspection is whether a data object is part of the "file" or an exhibit. The right to access data has been strengthened recently in Germany, when the Constitutional Court (Bundesverfassungsgericht) decided yearlong legal battles over the sharing of source data in speeding. The court held that defendants have, in principle, a right to inspect all data generated for fact-finding purposes [75].

---

[72] D. BRODOWSKI, *Strafprozessualer Zugriff auf E-Mail-Kommunikation*, in *Juristische Rundschau (JR)*, 2009, p. 407.

[73] See the wording of Section 147(1) GCPC: «Defence counsel shall have authority to inspect files which are available to the court or which will have to be submitted to the court if charges are preferred, as well as to view officially impounded pieces of evidence».

[74] See M. BOHLANDER, *German Criminal Procedure*, cit., p. 63.

[75] Bundesverfassungsgericht, Decision of 12.11.2020 (2 BvR 1616/18), available at "https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/11/rk20201112_2bvr161618.html;jsessionid=2C555F8F4A9974169D95EFD4D407B7F7.2_cid377".

4.2.1. *Right to Access the File by Defense Counsel*

The basic rule is that the lawyer, but not the defendant, has a comprehensive right to inspect the file that the prosecution has submitted to the court (or that would have to be submitted in case of indictment), including any «officially impounded pieces of evidence». The inspection must be guaranteed once the prosecution terminates the investigation stage and either proceeds to indictment or discontinuation of the case. Before this point in time, the prosecution may restrict the right to access, i.e. defense counsel can be refused inspection of the files or of individual parts of the files, as well as inspection of officially impounded pieces of evidence, insofar as this may endanger the purpose of the investigation [76]. If this restriction ground ceases to apply, the defense counsel has to be notified and may then have full access to the dossier (again) [77]. Beyond this ground for restriction, law enforcement authorities cannot hold back investigative findings. The right to access the file is accompanied by the principles of completeness of the file (*Aktenvollständigkeit*) and truthfulness of the file (*Aktenwahrheit*) [78].

The notion of a "file" is interpreted widely. It must contain all documents and records of technical nature, which may have relevance for the conviction and/or sentence [79]. It also includes computer data, data files established during the investigation phases, and computer printouts of data if they are relevant for the trial [80]. If law enforcement authorities selected and compiled data, the access right includes inspection of the data set which the compilation was based on [81]. As mentioned, German law distinguishes between the right to inspect the file and the right to view "exhibits". The latter is seen as a supplementary right, not as the genuine defendant's right

[76] Section 147 Subsection 2 Sentence 1 GCPC. Note also that an exception of this restriction is made if the defendant is in detention (Section 147 Subsection 2, Sentence 2): «(...) if the accused is in remand detention or if, in the case of provisional arrest, this has been requested, information of relevance for the assessment of the lawfulness of such deprivation of liberty shall be made available to defence counsel in suitable form; to this extent, as a rule, inspection of the files shall be granted».

[77] M. Bohlander, *German Criminal Procedure*, cit., p. 63.

[78] L. Meyer-Goßner-B. Schmitt, *Strafprozessordnung*, cit., § 147, mn. 14.

[79] J. Wessing, *Kommentierung des § 147*, in J.-P. Graf, *BeckOK StPO*, 35th ed., C.H. Beck, München, 2019, § 147, mn. 15.

[80] J. Wessing, *ibidem*.

[81] J. Wessing, *ibidem*.

to file access [82]. The effects of the difference mainly lay in the modus operandi of inspection [83]. Whereas the counsel can apply to take the file to her office for inspection (unless there are serious grounds for refusal), she is not entitled to do so as far as «officially impounded pieces of evidence» are concerned ("ban on handing over exhibits"). "Exhibits" cannot leave official custody and can only be viewed in the rooms of the judicial authority [84].

In the area of digital evidence, however, it is not always clear when "data" is part of the file or must be regarded as an «officially impounded piece of evidence». It is observed that both practice and legal literature often do not make the necessary distinctions as foreseen by law [85]. Often a precise differentiation is not made between the storage medium and the data stored on it, or between original data and data copies [86]. The main reason seems to be that the "right to inspect the file" (Section 147 GCPC) does not include specific rules on "digital evidence" – as we have seen in relation to the rules on search and seizure. The main criterion seems to be whether the authenticity of a piece of evidence must be maintained (and then exhibited) or not [87]. If there is a risk that the evidentiary value of a piece of evidence may be manipulated or falsified, the "object" must be regarded as an exhibit [88]. The "image", i.e. the copy of an original data set, for instance, is to be regarded as an «officially impounded piece of evidence». Likewise, child pornographic pictures on computers are assigned as exhibits. According to case law, assignment of these pictures as exhibits is not changed if the data has been "converted", e.g. visualized by printing or scanning [89]. Many problems are unsolved if it comes to

---

[82] L. MEYER-GOßNER-B. SCHMITT, *Strafprozessordnung*, cit., § 147, mn. 19.

[83] This is regulated in Section 32f GCPC. The provision is without prejudice to the right to inspect the files and to view the exhibits. Section 32f distinguishes the inspection of electronic files and inspection of files which are available in paper form.

[84] G. WILLNOW, *Kommentierung des § 147*, in R. HANNICH, *Karlsruher Kommentar zur Strafprozessordnung*, 8th ed., C.H. Beck, München, 2019, § 147, mn. 10.

[85] A. BELL, *Beschlagnahme und Akteneinsicht bei elektronischen Medien*, Dr. Kovac, Hamburg, 2016, p. 4.

[86] A. BELL, *ibidem*.

[87] L. MEYER-GOßNER-B. SCHMITT, *Strafverteidiger-Forum (StraFo)*, cit., § 147, mn. 19.

[88] D. WÖLKY, *Beschränkung der Verteidigung durch Einschränkung des Akteneinsichtsrechts*, in *Strafverteidiger-Forum (StraFo),* 2013, p. 493, at 496.

[89] OLG Frankfurt a.M., Decision of 2. November 2012 – 2 Ws 114/12, in *Neue*

records of intercepted telecommunication data (often entailing huge amounts of data) [90].

4.2.2. *Right to Access the File by the Defendant without Defense Counsel*

The German legislator recently aligned the right to access the file by a defendant who has no defense counsel to that of a defendant with defense counsel. In principle, after the reform of 2018 all defendants have a right to the inspection of the file and of the officially impounded pieces of evidence corresponding. Nonetheless, the rights of the defendant who has no defense counsel are still limited: The access to the defendant who has no defense counsel is only warranted if it cannot endanger the purpose of the investigation – also in another criminal proceeding – and the overriding interests of third persons meriting protection do not present an obstacle [91]. Furthermore, inspection of officially impounded pieces of evidence is only possible "under supervision". If files are not kept electronically, the defendant can inspect the files in the offices of the judicial administration or he can receive a copy of the file [92]. Legal literature criticizes this regime for not fully providing equal rights to a defendant who has a defense counsel and a defendant who does not [93].

4.3. *Remedies against Investigative Measures in Relation to Digital Evidence*

Again, the distinction between investigative measures that were

---

Juristische Wochenschrift (NJW), 2013, 1107, 1109 (Ger.); scholars, however, oppose this view (see the references at L. Meyer-Goßner-B. Schmitt, *Strafprozessordnung*, cit., § 147, mn. 19).

[90] Cf. A. Mosbacher, *Aktuelles Strafprozessrecht*, in *Juristische Schulung (JuS)*, 2017, p. 127; L. Meyer-Goßner-B. Schmitt, *Strafprozessordnung*, cit., § 147 mn. 19c-19d. In practice, the data storage media – in particular, the recordings of the telecommunication surveillance – are regularly not part of the file. They can only be perceived as pieces of evidence. A data transfer to the defence counsel (*e.g.* on a lawyer's mobile hard disk) is only made in exceptional cases. In these cases, the state criminal police office regularly establishes a "time lock", *i.e.* data can no longer be viewed after a certain period of time has elapsed.

[91] Section 147 Subsection 4 GCPC.

[92] Section 147 Subsection 4, Sentence 2 GCPC.

[93] W. Beulke-S. Swoboda, *Strafprozessrecht*, cit., mn. 245.

conducted covertly and those conducted openly determines which remedy a defendant can avail himself to in criminal procedure. An interesting question refers to remedies that the defendant can already exercise in the pre-trial stage of criminal proceedings.

4.3.1. *Covert Investigative Measures*

Explicit regulation exists for clandestine investigative measures, e.g. source telecommunication surveillance or online searches. Section 101 Subsection 7 GCPC stipulates that even after completion of the measure and for up to two weeks following their notification, the persons named in subsection (4), first sentence [94], may apply to the competent court that ordered the measure for a review of the lawfulness of the measure, as well as of the manner and means of its implementation. An immediate complaint (*Beschwerde* [95]) against the decision shall be admissible. Where public charges have been preferred and the accused has been notified, the court seized of the matter shall decide upon the application in its concluding decision.

Depending on the competences for the judicial order, different courts may be involved in this remedy system pursuant to Section 101 Subsection 7 GCPC. In conventional cases, the investigative judge at the local court (*Ermittlungsrichter am Amtsgericht*) orders an interception of telecommunications (Section 100a GCPC), and he/she also decides on the review of this measure if the application is made in the pre-trial stage before public charges are preferred. The regional court (*Landgericht*) is competent to decide on the complaint in these cases. Since online searches are ordered by a specific chamber of the regional court, this chamber will also decide on the review at first instance during the pre-trial stage. The complaint is decided by the Higher Regional Court (*Oberlandesgericht*). These competences can change if public charges have been preferred.

---

[94] As mentioned above, subsection 4 of Section 101 GCPC defines the persons who are entitled to receive notifications for each covert investigative measure. This may include also other person than the "targeted person".

[95] Cf. M. BOHLANDER, *German Criminal Procedure*, cit., p. 251 who defines «Beschwerde» (usually translated as: "complaint") as «general appellate remedy, mainly for ancillary or interlocutory relief, but not against conviction and/or sentence».

4.3.2. *Other Coercive Measures, e.g. Search and Seizures*

Regarding non-covert investigative measures, such as the search and seizure of emails, the scheme of remedies is complicated. The legislator has not laid down specific rules providing for legal remedies in the pre-trial stage. Nonetheless, case law has strived for transparency and clarity in recent years, and thus strengthened the individual's fundamental right to access to the courts/effective legal remedy as guaranteed by Article 19(4) of the Basic Law. As a rule, the defendant has the right to judicial review against the investigative measure, both as far as its lawfulness (requirements of ordering the measure) and the manner and means of enforcement are concerned. However, competences of courts and appeal possibilities depend on whether the coercive measure is completed or not and whether it was ordered by the public prosecution service, the police or by the judge. By rule of thumb, all orders by the investigative judge can be reviewed by way of complaint («*Beschwerde*») to the next highest court [96]. Lawfulness and means and manner of enforcement of coercive measures that are based on decisions (i.e. in exigent circumstances) by the public prosecutor or the officials assisting it (e.g. the police) can be reviewed by the investigative judge [97]. Against the decision by the investigative judge, the complaint («*Beschwerde*») to the next highest court is admissible [98].

If the coercive measure is completed, the defendant must show a legitimate interest in bringing proceedings to the court (*Rechtsschutzinteresse*) [99]. Certain categories have developed under case law as to when this legitimate interest can be affirmed. These

---

[96] Section 304 GCPC.

[97] Section 98 Subsection 2, sentence 2 GCPC in direct or analogous application. Section 98 Subsection 2 GCPC [orders of seizure] reads as follows: (2) «An official who has seized an object without a court order shall apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may, at any time, apply for a court decision. The competence of the court shall be determined by Section 162. The person concerned may also submit the application to the local court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights».

[98] W. BEULKE-S. SWOBODA, *Strafprozessrecht*, cit., mn. 503.

[99] If Section 101 Subsection 7 GCPC applies, a legitimate interest need not be claimed. It is irrefutably presumed by the law.

include very invasive encroachments on fundamental rights, danger of recurrence, and claims of public liability. A defendant's interest in rehabilitation is generally not accepted by the courts. Case law has affirmed the basis for invasive encroachments on fundamental rights if searches of private or business premises take place but denied it in the case of seizure [100].

The use of digital evidence in the trial may also be subject to the defendant's remedies against the conviction or sentence. In these cases, the ordinary remedies – appeal on fact and law (*Berufung*) and appeal on points of law only (*Revision*) – apply [101]. In sum, it can be observed that German law, up to now, has not taken into account the specificities of digital evidence. Seemingly, the opinion is that general rules sufficiently regulate digital investigations.

5. *Admissibility of Digital Evidence at Trial*

As things stand today, the admissibility of digital evidence at the trial stage is also governed by general rules as German law lacks specific admissibility rules for digital evidence. Exclusion of evidence is the exception, breaking Germany's strong inquisitorial tradition entrenched in the truth-seeking mission of courts [102] that also is valid if evidence is obtained by using forensic IT methods [103]. Lacking systematic admissibility rules, German law, however, bans evidence in certain cases explicitly stipulated by law (*gesetzliche Beweisverwertungsverbote*) and in various other situations, established by case law, when the balancing of conflicting interests is in favor of excluding certain evidence (*nicht normierte Beweisverwertungsverbote*) [104].

---

[100] W. BEULKE-S. SWOBODA, *Strafprozessrecht*, cit., mn. 501 with further references.

[101] See M. BOHLANDER, *German Criminal Procedure*, cit., p. 251 et seq.

[102] See S. GLESS, *AI in the Courtroom*, cit., p. 218-9; T. WEIGEND, *The Potential to Secure a Fair Trial Through Evidence Exclusion: A German Perspective,* in S. GLESS-T. RICHTER (eds), *Do Exclusionary Rules Ensure a Fair Trial?*, Springer, Cham, 2019, p. 61-92 at p. 72 f.

[103] D. HEINSON, *IT-Forensik*, cit., p. 123; D. KOCHHEIM, *Cybercrime*, cit., mn. 1875.

[104] W. BEULKE-S. SWOBODA, *Strafprozessrecht*, cit., mn. 703 et seq.

5.1. *Exclusion of Evidence Stipulated in the Law*

Even if the exclusion of evidence is an exception, in theory, digital evidence might be prone to exclusion due to three issues: first, Germany's strong commitment to protect privacy and the resulting ban not to collect or use information transgressing the core area of private life; second, legal protections of confidentiality or of professional secrecy; and third, the rather narrow-meshed legal framework when evidence is moved between different criminal proceedings or between non-criminal and criminal proceedings.

5.1.1. *Ban from Using Evidence Concerning the Core Area of Privacy for Interception Measures*

Following up on the case law of the Federal Constitutional Court, German law protects the privacy of telecommunication in cases of interception (including source telecommunication surveillance and online searches). According to Section 100d, Subsection 1 GCPC even the recording of communications (i.e. the collection of evidence) is prohibited if – on the basis of a prognosis – there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired. If it cannot be excluded beforehand that information relating to the core area of the private conduct of life will also be recorded, such information acquired during the interception measure is excluded from use in trial (Section 100d, Subsection 2 GCPC). The ban is comprehensive, i.e. not only information that specifically relates to the core area of the private conduct of life is inadmissible, but all information that was collected by the measure [105]. Information obtained may not even be used as a mere clue (*Spurenansatz*) in investigative proceedings [106], and also encompasses information on exonerating circumstances. If data that relates to the core area of the private conduct of life is detected, it must immediately be deleted. The notion «core area of private conduct of life» is not defined by the law. In essence, it means that anybody must have the opportunity to express herself without fear of being monitored by government

[105] L. Meyer-Goßner-B. Schmitt, *Strafprozessordnung*, cit., §100d, mn. 6.

[106] Federal Constitutional Court (BVerfG), Decision of 12 October 2011 – 2 BvR 236/08, in *Neue Juristische Wochenschrift (NJW)*, 2012, 833, 838 (mn. 220) (Ger.); B. Vogel, *Country Report Germany,* cit., p. 529.

institutions. This includes, *inter alia*, communication and information about inner feelings or deep relationships. Protection includes, for instance, communications between persons sharing a special relationship of trust within the scope of this core area. This may concern family members or other very close friends, priests, crisis lines, criminal defense attorneys, or – in individual cases – doctors [107].

5.1.2. *Protection of Professional Secrets*

For both covert and open investigative measures, the taking of such measures as well as the use of information obtained by them is prohibited if information is produced with respect to which a person can refuse testimony on professional grounds (Section 160a in connection with Section 53 GCPC). The provision's purpose is that law enforcement authorities do not circumvent the possibilities to refuse testimony in a situation of a hearing or witness examination by other investigative measures [108]. The law distinguishes between unconditionally and conditionally protected persons. If information was confided in clergymen, defense counsels, lawyers [109], and members of parliament in their capacity, the information is privileged and use of the information is absolutely excluded. In other cases of confiding information in persons entitled to protect their professional secrets, e.g. notaries, certified public accountants, sworn auditors, tax consultants (*Steuerberater*) and tax representatives (*Steuerbevollmächtigte*), doctors, and journalists, the law only provides for a relative ban on the use of information. This means that the question is whether information obtained by the investigative measure involving such "conditionally protected persons" is subject to a proportionality test. In procedures not concerning a criminal offence of substantial significance, the interest in criminal prosecution does not usually prevail, and the use of evidence is prohibited. The protection, however, is lost (both for unconditionally and conditionally protected professionals) if certain facts give rise to the suspicion that the person who is entitled to refuse to testify participated in the offence or in handling stolen

[107] BVerfG, *ibidem*, 837; B. VOGEL, *Country Report Germany,* cit., p. 528.

[108] L. MEYER-GOßNER-B. SCHMITT, *Strafprozessordnung*, cit., § 160a, mn. 1.

[109] Including non-lawyer providers of legal services who have been admitted to a bar association.

data, aiding after the fact, obstruction of prosecution or punishment, or handling stolen goods [110]. Strengthened, special rules exist for the protection of information/communication involving the mentioned persons entitled to refuse testimony, where these relate to seizures (Section 97 GCPC) and online searches (Section 100d, Subsection 5 GCPC).

5.1.3. *Use of Digital Evidence in Other Proceedings*

The use of evidence in criminal cases – other than the one it has been obtained for [111] – is, in principle, possible under German procedural law. It is, however, very complicated. Various legal provisions regulate different scenarios. Again, a distinction is made between evidence collected by covert and open investigative measures. In addition, the law distinguishes between the use of data collected in the framework of other repressive criminal proceedings and the use of evidence collected in the course of administrative proceedings, such as police proceedings preventing a danger or tax cases.

Since a series of coercive measures, in particular, in the area of covert interception measures, such as telecommunication surveillance and online searches, is only admissible if there are factual indications for a specific serious criminal offence (as defined in a catalogue of offences – see *supra* 2.1.), the concept of "hypothetical surrogate measures" ("*hypothetischer Ersatzeingriff*") plays an important role. In this context, the German law provides two specific provisions [112]:

(1) According to Section 479, Subsection 2 in connection with Section 161, Subsection 3 GCPC, any personal data obtained on the basis of such a measure, which is only admissible where specified criminal offences are suspected, may only be used without the consent of the person affected by the measure for evidentiary purposes *in other criminal proceedings*, in respect of which the clearing up of the criminal offence could have been ordered pursuant to the GCPC. Translated to the surveillance of telecommunications

[110] Section 160a, Subsection 4 GCPC.

[111] "Use in other proceedings" means another offence in the procedural sense, i.e. an offence not substantively connected with the original criminal proceedings.

[112] W. Beulke-S. Swoboda, *Strafprozessrecht*, cit., mn. 360 ff.

pursuant to Section 100a GCPC, for instance, this means that information containing personal data gained by the telecommunications surveillance for a specific criminal proceeding may be used if the other criminal proceeding concerns one of the offences listed in Section 100a Subsection 2 GCPC and provided that the remaining prerequisites for an order are fulfilled. The wording «for evidentiary purposes» led to the debate on whether chance discoveries may be used at least as investigative clues in other criminal proceedings without the need for consent of the person concerned and without the prerequisites of an order being fulfilled. The prevailing opinion considers such use of the information as a clue without further restrictions admissible [113].

(2) Section 161 Subsection 3 GCPC regulates the reverse case, i.e. the use of information that was *gained in non-criminal proceedings* in criminal proceedings. The provision includes a similar rule to Section 479 Subsection 2 regarding investigative measures in the GCPC that can be ordered only for specific criminal offences. Accordingly, where measures pursuant to the GCPC are only admissible where the commission of particular criminal offences is suspected, personal data that has been obtained as a result of a corresponding (i.e. not necessarily identical) measure taken pursuant to another statute may be used as evidence in criminal proceedings without the consent of the person affected by the measure, only to clear up one of the criminal offences in respect of which such a measure could have been ordered to clear up the offence pursuant to this statute. The provision is mainly applicable for covert investigative methods. Also here, the prevailing opinion is that the information gained can be used as clue without the necessity of meeting the restrictions of Section 161 Subsection 3 GCPC [114]. Corresponding formal requirements of the measure, as stipulated in the GCPC, do not need to be fulfilled. Thus, if, for instance, the police are searching a flat in order to avert a danger, without doing this on the basis of a court order, the information obtained during the search may also be used in the criminal proceedings [115].

Specific provisions regulate the use of information obtained in tax

---

[113] P. WITTIG, *Kommentierung des § 477*, in J.-P. GRAF, *BeckOK StPO*, 36th ed., cit., § 477 mn. 5.

[114] K. SACKREUTHER, *Kommentierung des § 161*, in J.-P. GRAF, *BeckOK StPO*, 36th ed., cit., § 161 mn. 15.

[115] K. SACKREUTHER, *ibidem*.

cases in criminal proceedings. According to Section 393 Subsection 2 of the Fiscal Code [116], (digital) evidence obtained in tax proceedings is excluded from use if it was produced from an obligation of the taxpayer to disclose that he/she had no knowledge of criminal proceedings and the criminal proceedings related to an "ordinary" offence (*Allgemeindelikt*). According to Sentence 2 of the provision, this shall not apply to crimes for the prosecution of which there is a compelling public interest. By referring to Section 30 Subsection 4 Number 5 of the Fiscal Code, such compelling public interest shall be deemed to exist if:

- Felonies [117] or deliberate serious misdemeanors that aim to cause human injury or loss of life or that aim to cause damage to the state and its institutions are to be prosecuted;
- Economic crimes are to be prosecuted, which – in view of the method of their perpetration or the extent of the damage they cause – are likely to substantially disrupt the economic order or to substantially undermine general confidence in the integrity of business dealings or the orderly functioning of authorities and public institutions; or
- The criminal proceedings are necessary to correct publicly disseminated incorrect facts which are likely to substantially undermine confidence in the administration.

Section 393 Subsection 3 Fiscal Code provides for the use of material in the reverse case: Accordingly, findings which the revenue authority or the public prosecutor's office lawfully gained in the course of criminal investigations may be used in the taxation procedure. These shall also apply with respect to findings subject to the privacy of correspondence, posts and telecommunications, to the extent that the revenue authority legally obtained them in the course of their own criminal investigations or to the extent that information may be issued to the revenue authorities pursuant to the provisions of the Code of Criminal Procedure.

---

[116] This reads as follows: «Where, during criminal proceedings, the public prosecutor's office or the court learns from the tax records of facts or evidence which the taxpayer, in compliance with his obligations under tax law, revealed to the revenue authority before the initiation of criminal proceedings or in ignorance of the initiation of criminal proceedings, this knowledge may not be used against him for the prosecution of an act that is not a tax crime».

[117] Criminal acts punishable by a minimum sentence of one year's imprisonment.

5.2. *Exclusion of Evidence not Stipulated in the Law*

It is widely acknowledged that evidence may be excluded or must be disregarded, although an exclusionary rule is not explicitly stipulated in legal provisions [118]. As a starting point, it is important to know that there is no (general) rule that evidence that was collected/obtained by violation of the substantive and/or procedural rules is per se inadmissible. The correct way of handling unlawfully obtained evidence is subject to an extremely contentious debate. There is a myriad of academic papers and – sometimes contradictory – case law. In line with the focus of the DEVICES study on the practical applications, the following paragraphs briefly outline the main principles of the case law of the Federal Court of Justice and the Federal Constitutional Court regarding the question of admissibility of unlawfully obtained evidence. These principles also apply to digital evidence or IT forensic investigations.

Legal doctrine in Germany distinguishes whether an exclusion of evidence must be accepted if the evidence was wrongly collected (*unselbständiges Beweisverwertungsverbot*) or whether a piece of evidence was legally collected but cannot be used for the conviction (*selbständiges Beweisverwertungsverbot*). The latter often follows because the use of the piece of evidence violates human rights, as stipulated in the Basic Law, or infringes the fair trial principle as stipulated in Art. 6 ECHR [119]. The first category (*unselbständiges Beweisverwertungsverbot*) is frequently involved if it comes to digital evidence, in particular, because the method or the technical procedures that were used were unlawful [120].

Such cases include the prosecution service ordering a measure despite the absence of an exigent circumstance (*Gefahr im Verzug*), thus unlawfully circumventing the requirement of a court order. Another example is the ordering of a covert investigative measure, although the measure could not be legitimately ordered, because no serious offence, as provided by the catalogue, was given. A law enforcement officer may also act beyond the limits indicated in a search order of the court. In addition, a piece of evidence may have been obtained by violation of foreign law [121].

---

[118] For case law, see T. WEIGEND, *The Potential to Secure a Fair Trial*, cit., p. 88 f.

[119] D. HEINSON, *IT-Forensik*, cit., p. 124.

[120] D. HEINSON, *IT-Forensik*, cit., p. 125.

[121] For this case, see Federal Constitutional Court (BVerfG), Decision of 9

It is widely accepted that the basic concept of the German criminal procedure law – the principle of free evaluation of evidence – reaches its limits because the material truth cannot be established "at any price" [122].

However, the Federal Constitutional Court stresses, at the same time, that inadmissibility of evidence not explicitly provided for by law should be the exception, «requiring grounds to be given as it impairs the ascertainment of a substantively correct and fair decision» [123]. The favored approach of the Federal Court of Justice and the Federal Constitutional Court is a weighing up of the state interest for prosecution against the fundamental rights of the person affected, in particular, by taking into account the gravity of the offence and the importance of the violation in each individual case [124]. Although the approach taken by the jurisprudence is very casuistic, decisions are made on a case-by-case basis, and it is hard to predict whether an illegal collection of evidence will result in an exclusion of evidence. Some guidelines and premises have developed under case law that should be taken into account when assessing potential inadmissibility:

- Weighing up is only necessary if the provision that governed the collection of the evidence serves to protect the person concerned. Hence, the purpose of a procedural provision, which was violated, must safeguard the position of the defendant during the criminal proceedings [125];
- The seriousness of the breach of procedural law and the gravity of the alleged offence are of key significance for the weighing of interests;
- Furthermore, the encroachment's impact on fundamental rights of

November 2010 – 2 BvR 2101/09, in *Neue Juristische Wochenschrift (NJW)*, 2011, 2417 (Ger.), which had to decide whether a CD containing the data of bank customers of a foreign bank – which the German State has purchased from a former bank agent – could be used in tax evasion proceedings against taxpayers in Germany.

[122] Federal Court of Justice (BGH), Judgement of 14 June 1960 – 1 StR 683/59, in *Official Case Reports BGHSt* 14, 358, 365; Federal Court of Justice (BGH), Judgement of 26 July 2007 – 3 StR 104/07, in *Official Case Reports BGHSt* 52, 11, 17 (Ger.).

[123] Federal Constitutional Court (BVerfG), Decision of 7 December 2011 – 2 BvR 2500/09, in *Neue Juristische Wochenschrift (NJW)*, 2012, 907 (910, mn. 117) (Ger.).

[124] Federal Court of Justice (BGH), Judgement of 11 November 1998 – 3 StR 181–98, in *Neue Juristische Wochenschrift (NJW)*, 1999, 959 (961) (Ger.).

[125] Federal Court of Justice (BGH), Decision of 27 February 1992 – 5 StR 190/91, in *Official Case Reports BGHSt* 38, 214 (220) (Ger.).

the person concerned as well as the question of whether the piece of evidence could have been obtained without a breach of law must be taken into account. The latter reflects the idea of hypothetical courses of investigation (*hypothetische Ermittlungsverläufe*);

- Inadmissibility is affirmed if the violation of the legal provisions would lead to encouraging the unlawful taking of evidence. Hence, a ban on the admission of evidence may particularly be required after serious, deliberate, or objectively arbitrary breaches of the law, in which fundamental rights have been intentionally or systematically disregarded [126]. For this reason, case law increasingly requires the justification and documentation of investigative steps by the law enforcement authorities [127];
- According to the Federal Court of Justice, evidence cannot be admitted if «essential objective prerequisites» for the order are not fulfilled, e.g. if the suspicion of an offence defined in the catalogue of Section 100a Subsection 2 GCPC was obviously not given;
- Ultimately, the Federal Court of Justice applies proportionality considerations, i.e. the admissibility of evidence is more likely if the criminal offence at issue is of "substantial significance" and other investigative means would have been less likely to succeed or it would have been substantially more difficult to establish the facts [128].

In sum, one can state that the Federal Court of Justice follows a rather restrictive line to accept an exclusion of evidence [129]. Another important feature in this context is the so-called "objection solution" (*Widerspruchslösung*) developed by case law of the Federal Court of Justice. In several cases of possible exclusion, the court requires defense counsel to object to the use of evidence "in time" during

---

[126] Federal Constitutional Court (BVerfG), Decision of 7 December 2011 – 2 BvR 2500/09, in *Neue Juristische Wochenschrift (NJW)*, 2012, 907 (910, para. 117) (Ger.).

[127] Federal Constitutional Court (BVerfG), Judgement of 20 February 2001 – 2 BvR 1444/00, in *Official Case Reports BVerfGE* 103, 142 (160) (Ger.).

[128] Federal Court of Justice (BGH), Decision of 13 May 1996 – GSSt 1/96, in *Neue Juristische Wochenschrift (NJW)*, 1996, 2940 (Ger.); see also P. KÖPPEN, *Country Report Germany*, cit., p. 566.

[129] H. KUDLICH, *Wenn Sie sich keinen Anwalt leisten können, wird Ihnen einer gestellt*, in *Juristische Arbeitsblätter (JA)*, 2018, p. 792.

proceedings before the first instance court. "In time" refers to where, after evidence has been taken in each individual case, the law allows the defendant to add anything [130]. Jurisprudence also applies this rule to defendants who have no defense counsel if the defendant was sufficiently informed by the judge regarding the need for an objection and its consequences. If the defendant or his/her defense lawyer do not object in time, any argument on the exclusion of an individual piece of evidence will not be heard on appeal.

6. *Conclusions*

The outline of the German body of law regulating digital evidence revealed a lacuna that legislation in this area is widely underdeveloped. Instead, digital evidence is integrated into the existing regulatory framework: Germany lacks specific regulations and case law is often fragmentized by a case-by-case approach. The reasons for what could be called a vast under-regulation are unclear and probably manifold. First, scope and definition of "digital evidence" ("*digitale Beweismittel*") seem not to be clear and uniform. What can be established is that the notion is used in a broad sense, encompassing all personal and non-personal data as well as IT systems, as such. The question, therefore, rightly arises as to whether regulations are possible at all or whether there is at least the need to regulate only certain forms of digital evidence gathering.

Second, "digital evidence" is often used in the context of investigating and detecting cybercrime activities (e.g. identification of cybercriminals by searching for data tracks, understanding IT incidents, etc.), for which actually also the mentioned specific BSI guidelines were initially developed. This singles out the importance of data as evidence for "ordinary crimes", e.g. fraud or tax offences. The application and development of IT forensic procedures can be relevant for all crimes. Nonetheless, it is seen as a Herculean task to adopt rules for all possible types of evidence produced in digital forms.

A third reason is that "regulations on digital evidence" probably do not fit into the existing system of German criminal procedure. German procedure law follows the rule of strict forms of proof or *Strengbeweis*, which means that any form of digitally collected information must either be translated by witness or expert testimony

[130] Sec. 257 GCPC.

or be transmitted into documentary evidence or evidence conceivable by personal inspection. Digital evidence cannot be considered a separate legal category of evidence. In this context, IT forensic methods can only have a supportive function, without the need for specific regulations. In addition, the German law does make distinctions between covert, long-term investigative measures of interception and open, short-term investigative measures, such as search and seizures. Both forms of investigative measures are considered as the most relevant actions to collect "digital evidence". Whereas the legislator, however, regulated the interception measures in a more or less specific way (due to constitutional law reasons), the open measures stick to the classic operations in the analogue world. Nonetheless, it seems that courts and doctrine have adapted with the situation to make these conventional measures designed for tangible "papers" applicable to intangible data.

With ambient intelligent environments becoming an increasing part of everyday life and IT systems surrounding and monitoring us, it is high time for the German lawmaker to address issues of digital evidence in more coherent legislation that ensures trustworthy and fair fact-finding.

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.

Katalin Ligeti-Gavin Robinson

THE HANDLING OF DIGITAL EVIDENCE IN LUXEMBOURG

1. *The legal framework* [1]

In Luxembourg law there is no explicit regulation of digital forensic procedures in relation to criminal proceedings. Digital forensic procedures are carried out on the basis of horizontal, technology-neutral provisions in legislation and common law. This is the case, most significantly, for the seizure of electronic data – although as discussed in more detail below, the relevant legal basis in the *Code de procédure pénale* ("CPP") was notably adapted in 2014 in order to better meet the challenges of seizing data.

Insofar as digital forensic procedures involve personal data [2], the processing of such data is subject to the provisions of the EU's

[1] In Luxembourg, virtually all legislation, jurisprudence, doctrine and commentary is in French. All translations in this report are the authors' own.

[2] As noted in *Guidelines on Digital Forensic Procedures for OLAF Staff,* 15 February 2016, p. 1: "As digital forensic operations often involve the collection of large amounts of data, including personal data, they may be privacy invasive. These

so-called "Law Enforcement Directive"[3] (hereinafter "LED"), as implemented in Luxembourg in 2018[4]. The new domestic rules apply broadly to the "processing" – implemented identically broadly as in the LED[5] – of personal data by the police and judicial authorities in the course of their core functions: the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The compliance of police and judicial actors with the implementing law will be monitored by both the national data protection authority (the *Commission nationale pour la protection des données,* "CNPD") and a newly-created, specialised *Autorité de contrôle judiciaire*[6]. Several principles, obligations and data subject rights found in the LED implementation are of direct or indirect relevance to manifold aspects of digital investigations, both in Phase One ("Acquisitive process") and Phase Two ("Investigative process") – for example, duties to keep a register of processing activities, along with rules on data security, retention periods, and informing data subjects of the processing of their data. The data protection legal framework will thus be referred to where appropriate in the ensuing sections.

In relation to administrative punitive proceedings in taxation matters, there is no explicit regulation of digital forensic procedures.

Desk research detected no specific guidelines, best practice or other soft regulations in relation to either criminal proceedings or administrative punitive proceedings. This finding was confirmed insofar as criminal proceedings are concerned at interview with members of the specialised "New Technologies" unit of the judicial

---

Guidelines are therefore also designed to help ensure compliance with data protection provisions in the context of digital forensic operations".

[3] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89.

[4] Law of 1st August 2018, Mémorial A N° 689, 16 August 2018 (hereinafter "LED Implementation Law").

[5] «"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction»; see Article 3(2) LED, and Article 2(1)2°, LED Implementation Law.

[6] Chapter 6, LED Implementation Law.

police (*Section nouvelles technologies,* hereinafter "SNT"), who are called upon to provide operational support to criminal investigators in all matters of digital evidence requiring technical expertise.

1.1. *Constitutional framework*

Although none have been specifically elaborated with regard to digital data or to protect the digital sphere, a wide range of constitutional principles may apply to digital investigations during Phase One or Phase Two, depending on the circumstances of the investigation or proceedings. There is no constitutional provision explicitly guaranteeing citizens a fair trial, but several articles of the Luxembourg Constitution contribute to the fulfilment of that fundamental principle [7]; notably, the granting to ordinary courts of exclusive jurisdiction over disputes related to civil liberties [8], the requirement that any court or tribunal must be established by law [9], the duty upon judges to state reasons and to pronounce judgments in public [10], and the independence of the judiciary vis-à-vis government [11].

All of these principles shape the pre-trial and trial stages of criminal proceedings wherein digital evidence is admitted and evaluated, and as such touch directly the "presentation" stage of Phase Two. Additionally, multiple stages of both Phase One ("identification", "collection") and Phase Two ("examination and analysis", "interpretation") are typically either handled or reviewed – in the standard judicial inquiry context – pre-trial by the investigating judge (*juge d'instruction*), who is independent and impartial by design, before the pre-trial chambers.

With respect to the lawfulness of search and seizure in the course of digital investigations, the key operative provisions in the CPP empowering police and judicial actors are conceived to be exceptions to the constitutional baseline of the inviolability of the

---

[7] V. Covolo, *Luxembourg*, in S. Allegrezza-V. Covolo (eds.), *Effective Defence Rights in Criminal Proceedings. A European and Comparative Study on Judicial Remedies*, Wolters Kluwer-CEDAM, Milan, 2019, p. 329 f.

[8] Article 84, Luxembourg Constitution.

[9] Articles 13 and 86, Luxembourg Constitution.

[10] Articles 88 and 89, Luxembourg Constitution.

[11] Article 93, Luxembourg Constitution.

home (*domicile*) unless prescribed by law [12] and the confidentiality of all communications [13].

The rights of the defence, although absent from the Constitution, were attached to Article 12 thereof [14] by the Constitutional Court in a 2013 judgment [15]. Furthermore, since Luxembourg follows the monist tradition regarding the status of international treaties in domestic law [16], Luxembourg judges give direct effect to individual rights featured in the ECHR as well as to EU Directives, which prevail over national legal provisions [17]. Key examples of European influence on Luxembourg domestic law in the digital investigations context are the right to access to a lawyer [18], and the request to annul evidence which has been illegally or improperly obtained which may be founded – according to jurisprudence tracing back to 2012 – on alleged violations of the right to a fair trial guaranteed by Article 6 of the ECHR [19]. The latter exclusionary rule and the effect thereupon of ECtHR case law are further discussed below, in particular in Section 4.

---

[12] Article 15, Luxembourg Constitution.

[13] Article 28, Luxembourg Constitution, reinforced and modernised by provisions of the Criminal Code (esp. Article 509-3(2)) and in other secondary legislation. See further V. FRANSSEN-K. LIGETI, *The cooperation of Internet and other service providers with judicial authorities: National report on Luxembourg*, in *Project Towards Polish Cybercrime Centre of Excellence* (Nicolaus Copernicus University Cybercrime Research Centre) 2015, p. 9. Available at *cybercrime.umk.pl/national-reports,26,en.html.*

[14] Article 12 provides that «No-one may be *poursuivi* – pursued/prosecuted — other than in cases foreseen by the law and in the form prescribed by the law».

[15] C. const. (*Cour constitutionnelle*), 25 October 2013, decision n° 104/13 in *Jurisprudence* database; available at *justice.public.lu/fr/jurisprudence.html.*

[16] See J. GERKRATH, *The Constitution of Luxembourg in the Context of EU and International Law as 'Higher Law'*, in A. ALBI-S. BARDUTZKY (eds.), *National Constitutions in European and Global Governance: Democracy, Rights, the Rule of Law*, Asser Press, The Hague, 2019.

[17] M. PETSCHKO-M. SCHILTZ-S. TOSZA, *Luxembourg*, in K. LIGETI (ed.), *Toward a Prosecutor for the European Union, Vol. 1,* Hart Publishing, Oxford, 2013, p. 450.

[18] Explaining the interplay in Luxembourg law between ECtHR jurisprudence, EU Directive 2013/48/EU and the reform of the CPP, see V. COVOLO, *Report on Luxembourg*, in S. RUGGIERI-S. QUATTROCOLO (eds.), *Personal Participation in Criminal Proceedings: A Comparative Study of Participatory Safeguards and in absentia Trials in Europe*, Springer, 2019, p. 280 f.

[19] Ch. c. C. (*Chambre du conseil de la Cour d'appel*), 16 May 2012, n° 301/12, in *Jurisprudence*; Ch. c. C. 22 October 2012, n° 674/12, in *Jurisprudence*.

1.2. *Administrative punitive proceedings*

Turning to administrative punitive proceedings, it ought first to be noted that no such concept is explicitly recognised in the Luxembourg legal framework. Doctrine and jurisprudence have, on the other hand, lengthily examined so-called "administrative sanctions" and the application – at times, adaptation – of constitutional principles such as that of the *légalité des peines* [20] to their somewhat anomalous [21] existence. Although as noted above the right to a fair trial is neither a constitutional principle nor codified in Luxembourg law, with regard to administrative sanctions such a right has been anchored in domestic legislation [22] and gradually refined in jurisprudence via references to the ECHR and to Strasbourg case law, including that flowing from the *Engel* judgment in 1976 [23]. Thus reflecting the Luxembourgish blend of constitutional principles and ECHR sources, in the doctrine it is settled that «the legality of the criminalisation, the legality of the sanction, the respect of defence rights, and the *recours en pleine juridiction*» [24] must be respected in the context of administrative sanctions.

The rights of the defence of the *administré* are addressed through general rules aiming to ensure «to the greatest degree possible the participation of the *administré* in the taking of administrative decisions (... including through) the procedural collaboration of the administration, the right of the *administré* to be heard and to obtain the administrative dossier, (and) the necessary justification of

---

[20] Article 14 of the Luxembourg Constitution provides that sanctions may only be established or applied by a (sufficiently clear) law. Describing how the latter principle has been "attenuated" when applied to administrative sanctions, see M. THEWES, *Quel régime juridique pour les sanctions administratives ?*, in *Revue des Tribunaux Luxembourg,* 2017, n° 2, p. 39 and the sources cited therein.

[21] Article 49 of the Luxembourg Constitution provides that «justice is served in the name of the Grand Duke by the courts and tribunals». Administrative sanctions necessarily represent an exception to this (exclusive) provision.

[22] Law of 1 December 1978 and Grand-Ducal Regulation of 8 June 1979 on administrative proceedings; respectively Mémorial A n° 87, 27 December 1978 and Mémorial A n° 54, 6 July 1979.

[23] M. THEWES, *Quel régime juridique pour les sanctions administratives?*, cit., p. 40.

[24] G. WIVENES, *Les sanctions administratives au Luxembourg – Contribution du Conseil d'État*, in *Les sanctions administratives en Belgique, au Luxembourg et aux Pays-Bas, Analyse comparée*, Meeting of State Councils of Benelux and the Administrative Court of Luxembourg, Brussels, 21st October 2011, available at *raadvst-consetat.be/?action=doc&doc=929*, p. 24.

administrative acts» [25]. Naturally, some aspects of this framework sit awkwardly with the very dynamic of taxation. Accordingly, the standard rules do not apply to direct taxation [26], which remains governed by the amended *Abgabenordung* (hereinafter, "AO") from 1931 [27]; whilst they do apply to VAT, the horizontal framework is supplemented by sectoral rules [28].

In line with Strasbourg jurisprudence unequivocally recognising tax penalties as capable of having a "criminal" nature [29], and necessitating ultimate recourse to a tribunal fulfilling the conditions of Article 6 of the Convention, tax penalties may be appealed against to the Administrative Court (for direct taxes) [30] or to the District Court of Luxembourg «sitting in civil matters» [31].

Lastly, for overall understanding of this national report it is worth highlighting that although the precise situation regarding the "criminal" nature of tax fraud offences in domestic law was significantly less clear beforehand [32], since a sweeping tax reform in

---

[25] Article 1, Law of 1 December 1978.

[26] Article 5, Law of 1 December 1978. Concerning taxation *per se*, provisions of the Luxembourg Constitution are no more than foundational: no state tax may be established without a law; state taxes are voted annually; and no privilege in tax matters may be established (although exemptions and moderations can be established by a law): known as *l'égalité devant l'impôt* (Arts. 99-101, Luxembourg Constitution). See also ECHR, 12 July 2001, Ferrazzini v. Italy, wherein the Grand Chamber found that tax proceedings do not fall under the «civil rights and obligations» head of Article 6 of the Convention; §§ 29-31. The applicant had alleged that tax proceedings had exceeded a "reasonable time".

[27] Abgabenordnung Vom 22. Mai 1931 (Loi générale des impôts du 22 mai 1931), Mémorial A900 ("General Tax Law").

[28] Law of 12 February 1979 concerning VAT ("VAT Law"); Law of 10 August 2018 and Grand-Ducal Regulation of 5 December 2018 on the organisation of the *Administration de l'enregistrement, des domaines et de la TVA* ("the VAT Administration"). See A. STEICHEN, *Manuel de droit fiscal. Droit fiscal général,* 5th ed., Éditions Saint Paul, Luxembourg, 2015, noting that Luxembourg courts sometimes do not apply the Law of 1 December 1978 and the Grand-Ducal Regulation of 8 June 1979, citing the allegedly special nature of VAT; p. 136 f.

[29] ECHR, 23 November 2006, Jussila v Finland, §§ 30-31, 37-38; ECHR, 10 February 2015, Österlund v. Finland, §§ 35-39.

[30] Article 8, Law of 7 November 1996 on the organisation of the administrative jurisdictions, Mémorial A n° 79, 19 November 1996.

[31] Article 79, VAT Law.

[32] See M. MARTY, *La répression pénale transfrontière de la fraude à la TVA dans l'Union Européenne*, in C. HERBAIN (ed.), *La fraude à la TVA,* Promoculture Larcier, Windhof, 2017, challenging (p. 312) the recurring use in the doctrine of both "decriminalisation" and "administrative sanction" in light of a Luxembourg District Court decision in 2002 affirming the competence of the *tribunaux répressifs* with

2017 an objective threshold-based division is now in place between the administrative offences of simple tax fraud and the criminal felonies (*délits*) of aggravated tax fraud and *escroquerie fiscale*. Simple tax fraud, which may be committed intentionally or involuntarily, attracts fines (*amendes fiscales*) issued by the relevant tax administration, which may be challenged first internally and then before the administrative courts. Aggravated tax fraud and *escroquerie fiscale* on the other hand, with regard to both direct taxation and VAT, attract imprisonment as well as fines and are, as criminal felonies, the domain of criminal investigators and of the repressive courts exclusively [33].

1.3. *Seizure, copies and deletion*

As noted at the very outset of this chapter, in Luxembourg the seizure of digital evidence is to a large extent regulated identically to the gathering of any other form of evidence. A notable exception is found in the changes made to the CPP by the 2014 law implementing the Budapest Convention and codifying certain baseline procedural steps for the seizure of stored content data by the investigating judge (in the typical scenario of the judicial inquiry), the public prosecutor (in the limited *mini-instruction* scenario, outlined in Section 2 below) or the judicial police (in urgent cases, as detailed further below) [34]. These adjustments include an express provision on the making of copies – rather than the seizure of physical electronic devices – and the enlisting of decryption experts. Still, there is no limitation with regard to either

---

regard to simple tax fraud, a *délit,* attracting therefore a *peine correctionnelle* rather than an administrative sanction; T. A. Lux. (*Tribunal d'arrondissement de et à Luxembourg*), 14 February 2002, n° 353/2002, in *Jurisprudence.*

[33] § 396(7), *Abgabenordnung*, cit. (for direct taxes); Art. 80(1), VAT Law as amended, cit. (for VAT).

[34] We refer here to the "digital seizure" of data, executed through devices encountered following the physical search (*perquisition*) of premises – i.e. investigators entering an office building, personal residence, data centre etc. This scenario stands in contrast to digital searches (*perquisitions informatiques;* in Germany, *Online-Durchsuchung*). In the absence of any provision in the CPP and given the impossibility of respecting even common law rules on search and seizure (for instance, the presence of the target or of witnesses), in Luxembourg such measures are not only considered illegal in a procedural sense but are also likely to constitute a criminal offence of fraudulent access and/or deployment of spyware, depending on the facts; J.-L. Putz, *Cybercriminalité. Criminalité informatique en droit luxembourgeois*, Larcier, Windhof, 2019, p. 244.

device type or data type in these broadly-termed powers: searches may be carried out in any place where objects may be found which could be useful for the discovery of the truth [35], and the investigating judge's powers of seizure are all-encompassing, covering *inter alia* any object, document, effects, data stored, processed or transmitted in an automated data processing or transmission system [36]. In practice, it appears that when a copy of seized data is made, in general the data are saved on CDs, DVDs, hard drives or even (less secure) USB sticks depending on the volume of data to be seized [37].

Agents of the VAT Administration enjoy broad powers to consult (and potentially seize) documents and records [38], without any specifications as to types of devices and data.

There are no tailored legal requirements to be met in order to open a digital investigation in the context of criminal proceedings. However, as mentioned above, some modifications to the seizure powers in the CPP were made by the Law of 18th July 2014 [39] implementing the Budapest Convention in Luxembourg law which do represent significant conditions. An express reference to data was inserted into the CPP provisions where none had previously existed; until then, the seizure of data was nonetheless carried out in practice on the basis of the existing texts [40], despite their unequivocal emphasis on physical objects. As such, the Budapest reform added a measure of legal certainty to the process of seizing digital evidence – without tackling in detail the question of ensuring its authenticity and integrity.

---

[35] Article 65, Luxembourg Code de procédure pénale.

[36] Article 66(1), Luxembourg *Code de procédure pénale.* The power also covers effects which have been used to commit the crime or which were destined to be used as such and those which have formed the object of the crime, as well as everything which appears to have been the product of the crime, as well as in general, all that appears useful to the discovery of the truth or the use of which would be of such as nature as to harm the good workings of the *instruction* and all that is liable to confiscation or restitution (Article 31(3)).

[37] J.-L. PUTZ, Cybercriminalité, cit., p. 264. See also Rapport d'évaluation sur le septième série d'évaluations mutuelles "Mise en *œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci" – Rapport sur le Luxembourg (Brussels, 19th May 2017),* (hereinafter "GENVAL Evaluation")*, p. 49. Available at data.consilium.europa.eu/doc/document/ST-7162-2017-REV-1-DCL-1/fr/pdf.*

[38] Article 70, VAT Law.

[39] Law of 18th July 2014, Mémorial A133.

[40] See M. BRAUN, La ratification de la Convention de Budapest sur la cybercriminalité par le Luxembourg, in Journal des tribunaux Luxembourg, 2014, No. 35, p. 132 and the jurisprudence cited therein.

Since the reform, it is established in the CPP that seizure of data can be done either by taking possession of the device (*support physique*) or by making a copy of the data made in the presence of the persons attending the search [41]. The express possibility to copy data in the context of a seizure was inserted in the CPP by the 2014 reform in order to assuage the complexities involved in seizing immaterial data effectively and proportionately. For instance, where the targeted data are stored on a server along with the data of other persons who are not the subject of the judicial order, seizing the entire server would impact third parties [42]. Furthermore, the sought data might be found on the device of an "operator" who is not targeted by the preliminary investigation or judicial inquiry. Being able to make a copy of the data means there is no need to seize the object of a third party (necessitating in turn a fresh investigation or *instruction*) [43].

If a copy is made, the investigating judge may order the definitive erasure of the data on the device, where the device is located in Luxembourg and is not "in the hands of justice", and where possession or use of the data is illegal or dangerous for the security of persons or goods [44]. By doing so, the further commission of various cybercrime offences can be prevented – from hacking offences to possession or distribution of illegal content such as child sexual abuse material [45]. What is perhaps not immediately apparent from the wording of the provision is that in order to erase data, a copy *must* first be made. Apart from facilitating future use of the data as evidence, the existence of a copy is required in case the erasure decision is successfully challenged before the pre-trial chamber or at trial, or in case proceedings are discontinued or end in acquittal [46]. Should no copy of (legal) data remain, their restitution would be impossible.

In the VAT field, there are no specific requirements for digital

---

[41] Article 66(3), Luxembourg *Code de procédure pénale.*

[42] M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 132. Servers may furthermore often be so large as to "fill entire rooms", rendering physical seizure of hard disks impossible; see *Projet de loi* n° 6514, *Rapport de la commission,* p. 12.

[43] *Ibidem*.

[44] Article 66(3), Luxembourg *Code de procédure pénale.*

[45] M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 132.

[46] See M. BRAUN, *ibidem,* noting (p. 132) that the *Conseil d'État* had raised this issue in its first opinion on the Bill which was to become the Law of 18th July 2014, from 16th July 2013, *Doc. parl.* no. 6514-2, p.6, point 4.

investigations. Broad powers exist in order to compel the "communication" of sundry records to the agents of the VAT Administration [47]. On closer reading, "communication" of records does not seem to imply physical distance, since the general rule provides that all such documents are to be consulted on site (*sur place*), and may only be removed by agents with the agreement of those concerned [48]. That general rule is confronted, however, by an exception for bills and other documents which prove an offence or establish or support the establishment of a tax or a fine – which may be kept by agents to be joined to their reports (*procès-verbaux*). In turn, that exception does not cover commercial records (*livres commerciaux*) [49]. Finally, Article 70(3) provides: «When books, documents and, generally, all data, which must be communicated on request of the Administration, exist in electronic form, they must be, on request by the Administration, communicated in a form which is readable (*lisible*) and directly intelligible, certified to conform to the original, on paper, or following all other technical modalities determined by the Administration».

1.4. *Other investigative measures*

Returning to criminal proceedings but moving beyond measures of search and seizure, the live monitoring and acquisition of digital data with no communicative content may occur on the basis of several discrete investigative measures, all governed by the CPP.

First, Articles 88-1 to 88-4 of the CPP govern "special surveillance powers", comprising the interception of telecommunications and postal correspondence, along with (since a 2018 reform [50] which purposely mirrored developments in France and Belgium [51]) audio and visual surveillance in places and vehicles,

---

[47] Article 70(1), VAT Law.

[48] Article 70(1), para 3, VAT Law.

[49] Article 70(3), VAT Law.

[50] Law of 27 June 2018, Mémorial A559. The main changes in the 2018 reform are: a more flexible extension of 24-hour detention; undercover online investigations («*enquête sous pseudonyme par voie électronique»)*; searches of premises at any time of day or night; placement of devices in private premises in order to carry out audio or visual surveillance.

[51] *Exposé des motifs, Projet de loi* n° 6921, p. 7; see also the outcomes of the Council of Europe GENVAL Evaluations in 2017, cit., Recommendation n. 3 (of 9): «Luxembourg should reflect on adopting technical and legal tools to carry out

and a new "IT data capture" power [52]. The last two powers may enable the monitoring and acquisition of digital data with no communicative content in addition to digital data with communicative content. For instance, a camera hidden in a car may capture images of criminal activity and/or conversations between targets. The "IT data capture" power, similarly, may cover both types of data, seeing as it extends to «the placement of a technical device with the aim of accessing, without the consent of the persons involved, in any place, electronic data and recording, preserving and transmitting them, as they appear on a screen for the user of a system of automatic processing or transmission of data, as the user introduces them by inputting characters or as they are received and emitted by audiovisual peripheral devices» [53].

Whereas the interception of telecommunications is available in relation to criminal proceedings concerning «in whole or in part, an act of particular seriousness carrying a criminal or correctional sanction of at least two years' imprisonment» [54] – raising the possibility of its use in antifraud proceedings – recourse to audio and visual surveillance and "IT data capture" is very strictly trammelled in the CPP's detailed provisions both in terms of scope and procedure [55]. The latter powers are only available to the investigating judge in relation to a handful of serious terrorism-related crimes [56]. In other words, such constraints respond squarely to concerns around the intrusiveness of these measures rather than addressing the specificities of the digital evidence thereby gathered.

Secondly, another relevant investigative measure – which is by contrast available in antifraud cases given the lower sanction threshold of one year's imprisonment – is the power to "track and localise" telecommunications [57]. Again here, constraints both

---

infiltration operations and undercover investigations ("*enquêtes sous pseudonyme*") in cyberspace»; at 9.2.1 (authors' translation).

[52] Additionally, since 2018 undercover online investigations (*enquête sous pseudonyme par voie électronique*) are permitted in exceptional cases under Article 48-26 of the CPP.

[53] Article 88-1(3), Luxembourg *Code de procédure pénale.*

[54] Article 88-2(2)1°, Luxembourg *Code de procédure pénale.*

[55] For instance, exceptions and special safeguards are provided for individuals bound by professional secrecy, lawyers, doctors, professional journalists; see Article 88-2(6), Luxembourg *Code de procédure pénale* (and see further discussion below).

[56] Crimes and *délits* against state security and acts of terrorism and terrorist financing, when committed through electronic communications; Article 88-2(2)1°, Luxembourg *Code de procédure pénale.*

[57] Article 67-1, Luxembourg *Code de procédure pénale.*

personal (investigating judge only) and procedural (*inter alia* levels of justification, time limitations, record-keeping) are in place in order to calibrate proportionality, but without the specificities of digital evidence being addressed [58]. Attendant safeguards resemble those in place in the context of special surveillance measures (see above) but, reflecting a conviction that traffic data are far less sensitive than content, are distinctly less stringent. As opposed to the *décision spécialement motivée* required in the aforementioned cases, for "track and localise" the investigating judge merely indicates the factual circumstances of the case which justify the measures in an order giving reasons, which he communicates to the public prosecutor. Likewise, although he must specify the duration of application of the measure, which may not exceed one month – this is renewable, with no maximum period foreseen [59]. The 2014 Budapest reform law also made it possible for the public prosecutor to issue a request to an investigating judge for a "track and localise" order in the context of a *mini-instruction*, as such limited to certain specified *crimes* and felonies carrying a correctional penalty of a maximum of at least one year's imprisonment [60]. Prior to the reform, the need to resort to opening a judicial inquiry every time telecommunications data had to be tracked and localised had led to a

[58] Stepping away from the legal framework *stricto sensu,* in relation to both the interception of electronic communications and the "tracking and localisation" of telecommunications, procedural and technical specifications are provided rather at the regulatory level by the telecommunications regulator, the *Institut Luxembourgeois de Régulation* ("ILR"). Last updated in late 2017, these rules set the "national specifications" according to which regulated entities make "all forms of communications intercepted and related data" available to the investigating judge pursuant to the CPP provisions just mentioned. The ILR rules also oblige those entities to ensure readiness, timely response times, decryption (where feasible), security measures and confidentiality, and are thus of relevance to ensuring the integrity of digital evidence – at least on the cooperative private side of the equation. See *Règlement* ILR/T17/11 of 14 December 2017, Mémorial A – No. 13, 3 January 2018.

[59] Article 67-1(1), Luxembourg *Code de procédure pénale.*

[60] Similarly to the Belgian reform which inspired it, since 2010 the public prosecutor has been empowered to request that the investigating judge order a search of private premises, the hearing of a witness or an "expertise" without opening a judicial inquiry (*instruction préparatoire*), in relation to all felonies (*délits*) as well as certain specified crimes: use of forged documents, and theft with aggravating circumstances or with violence. Note that whilst the baseline *mini-instruction* facility applies to all *délits,* "track and localise" orders are not available for *délits* which do not carry a correctional penalty of at least a year's imprisonment; Article 24-1(1), Luxembourg *Code de procédure pénale.*

build-up of *procédures de non-lieu* (groundless proceedings) before the pre-trial chamber. Especially as concerns "track and localise" orders which produced no outcome, this created unnecessary and time-consuming formalities in unfruitful dossiers which the public prosecutor would have otherwise simply shelved [61].

Lastly as concerns digital data with no communicative content, "live" access to certain subscriber and use data held by electronic communications providers ('ECS') is provided via a new facility introduced by the Law of 27th June 2018. That law inserted a provision into the Law of 30th July 2005 (the Luxembourg implementation of the EU ePrivacy Directive) in order to further boost data-sharing by certain providers of ECS who are regulated by the *ILR* with that regulator, and ultimately with the public prosecutor or investigating judge, who both enjoy unfettered access (*accès de plein droit*) thereto [62]. By virtue of the new Article 10*bis* in the 2005 law, «Centralised register within the Institute», ECS providers which possess/use a Luxembourg dialling code (*en ayant recours à des ressources de numérotation luxembourgeoises*) shall:

«(2) (...) transmit automatically and free of charge to the Institute by electronic means and via a secure interface, the following data:

1. For natural persons: name, first name, habitual place of residence, date and place of birth along with the contact number of the subscriber;

for legal persons: denomination or business name (*raison sociale*), address of place of establishment along with a contact number;

2. The name of the regulated entity, the nature of the service provided by that entity, the call number allocated in relation to the service and, if available, the date of the end of the contractual relationship or in case of prepayment the deactivation date of the call number;

3. For natural persons, the type, the issuing country and the number of identification or proof of deposit of a request for international protection of the subscriber in cases of prepaid services».

It is worth underlining that although the *ILR* is the competent

---

[61] M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 133.

[62] The new Article 48-27 CPP also provides for a corollary cooperation duty on «telecommunications operators and telecommunications service providers» to provide access to *inter alia* prosecutors, investigating judges or (in urgent cases and subject to strict limits) to the police to data retained under art. 10*bis* of the 2005 law in order to identify subscribers, users or ECSs used.

regulator for ECS as broadly defined in the regulatory framework, since the above obligations refer to ECS with numbering/dialling codes attributed by the *ILR,* they apply only to telephony services [63]. The listed data must be updated at least once a day, even if there has been no change. Regulatory sanctions apply to any provider who should fail to meet their obligations under the scheme. The register was due to be implemented within a year of the entry into force of the modified law, although a *Règlement Grand-Ducal* setting out technical requirements was published in December 2018 [64], at the time of writing (July 2020) it has not been possible to confirm whether the register is now live – but this would seem probable [65].

Direct access to the data held in the central register by the ILR is regulated in Article 10*bis*(4) of the 2005 law which provides:

«(4) The public prosecutor, the investigating judge and the officers of the judicial police referred to in article 10 of the CPP acting on the basis of Article 48-27(1) CPP, as well as the state intelligence service have full and free access (*accèdent de plein droit*) to the register referred to in paragraph 1. Full and free access is limited to the measures set out in Article 48-27 CPP and those taken on the basis of the Law of 5th July 2016 on the reorganisation of the state intelligence service».

Thus, in a recalibration inspired by Article 46*bis* of the Belgian *Code d'instruction criminelle* the relevant data are available virtually "on tap" for investigators, in relation to the investigation of all crimes and felonies, whether by requests sent to telecommunications providers (which fall outwith the scope of this research project) or by remote electronic access to the central register managed by the regulator (which may fall within "live acquisition").

No powers to engage in the live acquisition of content or non-content communications data are available to the tax authorities, competent in cases of simple tax fraud, whether in relation to direct taxes or VAT.

---

[63] In a note to professionals on its website, the *ILR* further explains that the duty covers services «which allow telephone calls, so that M2M services are excluded from the scope (...) and including resellers of fixed-line or mobile telephony services"; *web.ilr.lu/FR/Professionnels/Communications-electroniques/Numerotation/Fichier-centralise–-Authentification* (posted on 5th June 2019).

[64] ILR Règlement ILR/T18/12 du 5 décembre 2018.

[65] See for an introduction to the register, naming of the register as "IR.COM", and FAQ for market operators, the *ILR* note to professionals, 5th June 2019, cit.

1.5. *Flagrancy*

In urgent cases of *crime* or *délit flagrant,* meaning essentially when suspects are caught in the act of committing an offence or in the immediate aftermath [66], an officer of the judicial police may seize electronic devices as he would any object or document, subject to the essentially the same procedural steps regarding the making of copies and the deletion of data as outlined above in relation to a seizure ordered by the investigating judge [67]. This power is available in relation to all *crimes* and to felonies (*délits*) which carry the sanction of imprisonment [68].

In light of the broad scope and intrusiveness of the measure, which depends heavily on the subjective assessment of police officers, since 2006 Article 48-2 of the CPP provides that the public prosecutor as well as any person demonstrating a legitimate personal interest may request the annulment of (any act of) the preliminary investigation. This *ex post* judicial review – available on simple request – of preliminary investigations was introduced in order to protect the rights of those involved as well as to ensure early judicial scrutiny of investigative acts undertaken by the police that often lead to the opening of a judicial inquiry [69]. In the course of an interview with the SNT, our research team was informed that in practice an investigating judge is systematically alerted by telephone before seizures are carried out. In fact, in Luxembourg a system is in place ensuring that an investigating judge is available on call 24/7 partly in order to cater for such eventualities.

1.6. *Quick freeze, urgent expertise and decryption*

Since the 2014 reform mentioned above, the rapid preservation of data (so-called "quick freeze") [70] is foreseen in Article 48-25 of the CPP as follows:

---

[66] See Article 30, Luxembourg *Code de procédure pénale.* The scope of this provision may extend considerably in the context of a continuous crime (*infraction continue*), which gives rise to a permanent state of "flagrancy"; see e.g. Ch. c. C., 2 June 2014, N° 371/14, in *Jurisprudence*.

[67] Articles 31 and 33, Luxembourg *Code de procédure pénale*.

[68] Article 40, Luxembourg *Code de procédure pénale.*

[69] *Projet de loi* n° 5354, 30 June 2004, at 19.

[70] Article 48-25, Luxembourg *Code de procédure pénale.*

«When there are reasons to think that data stored, processed or transmitted in an automated data processing or data transmission system, which are useful to the discovery of the truth, are susceptible to being lost or modified, the State Prosecutor or the seized investigating judge may order the rapid and immediate preservation, for a period which may not exceed 90 days, of these data».

The "quick freeze" facility is thus a general provision which applies across the board for all types of data [71], and may be triggered by the public prosecutor or an investigating judge – in practice, either through the police or in person [72] – in the national context as well as following receipt of a request from a foreign competent authority [73]. Once the data is preserved by a service provider, seizure may be executed by investigators safe in the knowledge that the desired data is (temporarily) «protected from anything that would cause its current quality or condition to change or deteriorate» [74]. Although the adoption of a Grand-Ducal Regulation on "*divulgation rapide"* of traffic data had been envisaged in the Bill to become the Law of 18th July 2014 [75], no such instrument has yet materialised – but "quick thaw" of some amount of traffic data may nonetheless be common in practice, even in cross-border cases [76].

Under Article 87(9) CPP, the investigating judge may also order that an *expertise* be carried out urgently, without the *inculpé* present, where she has reason to fear the imminent disappearance of facts and clues which she deems useful to the discovery of the truth. The judicial order specifies the reason for such urgency. Although this provision applies to experts of all kinds, it is worth noting that since the Budapest Convention reform in 2014, mentioned above, the investigating judge may also order any person (other than the target of the investigation) «whom he considers to have particular knowledge of (a) system of automatic processing or transmission of

---

[71] Doc. parl. 6514, exposé des motifs, cit., p. 13.

[72] M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 131.

[73] Doc. parl. 6514, exposé des motifs, cit., p. 13.

[74] Explanatory Report to Budapest Convention, para 159.

[75] Doc. parl. 6514, exposé des motifs, cit., p. 13.

[76] A leading practitioner has argued that the rapid release of traffic data in the Budapest Convention constitutes an "autonomous procedure" of direct transmission between authorities across national borders of State Parties to the Convention "without any other formalities"; see M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 131.

data or of the protection or encryption mechanism, to give him access to the seized system, to the seized data contained within the system or accessible from the system, as well as to the understanding of the seized or encrypted data» [77].

No specific rules focused on urgency were detected in the VAT context, but an exceptional power enables agents of the VAT Administration to access professional premises such as headquarters, offices, factories, shops, storage halls and so on at any time of day or night where there exist «sufficient serious indications or legitimate reasons permitting (agents) to consider that an inspection of respect of the legal dispositions applicable in VAT matters is necessary» [78]. The standard rule permits access only during the hours of professional activity [79].

1.7. *Proportionality: rules, challenges and best procedure*

There are no proportionality requirements which apply uniquely to digital criminal investigations. Yet necessity and proportionality requirements are inherent firstly in constraints placed on the relevant actors i.e. the investigating judge or public prosecutor. Most importantly, the investigating judge (who has a near-monopoly on coercive measures) uses her powers [80] – such as searches [81] and seizures [82] – in order to "discover the truth", meaning in a scrupulously even-handed manner (*à charge et à décharge*) [83]. Although her freedom to exercise her powers are in principle subject to no restriction [84], some objective procedural limits are in place; for example, other than in urgent cases of *infraction flagrante* or for a handful of terrorism-related crimes, searches must not take place after midnight and before 6am, on pain of nullity [85].

---

[77] Article 66(4), Luxembourg *Code de procédure pénale.*

[78] Article 71, VAT Law.

[79] *Ibidem*.

[80] So long as the investigating judge is "seized" correctly by the Public Prosecutor, she is obliged to carry out *actes d'instruction,* such as searches and seizures; Ch. c. C., 9 July 2013, n° 375/13, in *Jurisprudence*.

[81] Article 65(1), Luxembourg *Code de procédure pénale.*

[82] Articles 66(1) and 31(3), Luxembourg *Code de procédure pénale.*

[83] Article 55(1), Luxembourg *Code de procédure pénale.*

[84] M. Franchimont-A. Jacobs-A. Masset, *Manuel de procédure pénale,* 4th ed., Larcier, Brussels, 2012, p. 517.

[85] Article 65(3), Luxembourg *Code de procédure pénale.*

Furthermore, whilst a search warrant need only indicate the goal of the search, this must not be so broad as to indicate that the investigating judge did not consider whether less intrusive measures would have sufficed. Luxembourg was notably held in 2013 to have violated Articles 8 and 10 of the ECHR after a police-only execution on journalists' offices of a search warrant which indicated, *inter alia,* «any documents and items, in whatever form and on whatever medium, connected with the offences charged» [86]. Although the investigating judge had of his own motion ordered the discontinuation of the seizure and the return of all documents and items seized during the search, his order was nonetheless subsequently upheld successively by both pre-trial chambers [87], before an application to Strasbourg was made.

Any act taken in the course of a judicial inquiry may be attacked in the first instance before the pre-trial chamber of the competent District Court, pursuant to Article 126 of the CPP (the procedure is discussed further in Section 4 below). The seizure of digital devices and/or of data has thus been examined in several sets of proceedings before the pre-trial chambers of the District Court of Luxembourg and of the Court of Appeal. In 2014, the pre-trial chamber of the Court of Appeal rejected a request by two companies to have searches and seizures carried out on their premises annulled, alleging that the judicial order was drafted too broadly (the appellants complained of a "fishing expedition"), insufficiently targeted on the offences in respect of which the investigating judge had been seized (which included direct taxation offences), and "betrayed" partiality on the part of the investigating judge. Whilst the latter two claims were rejected summarily, it is the reasoning used by the chamber in rejecting the first complaint which interests us here. Parts of the wording used in the warrant (e.g. «everything concerning...»; «everything which permits....») were indeed excessively (and

[86] ECHR, 18 April 2013, Saint-Paul Luxembourg S.A. v. Luxembourg, § 59. Under the "most careful scrutiny" due for limitations on the confidentiality of journalistic sources (§ 58), the ECtHR considered that «the impugned search and seizure were disproportionate inasmuch as they enabled the police officers to search for the journalist's sources. The Court notes that the insertion of a USB memory stick into a computer is a procedure which can facilitate the retrieval of data from the computer's memory, thus supplying the authorities with information unrelated to the offence in question. The warrant (...) was not sufficiently narrow in scope to prevent possible abuse» (§ 61).

[87] §§ 17-21, *ivi.*

regrettably) broad, agreed the chamber, but they were superfluous as other operative wording met the required levels of precision («to identify the natural persons»; «to identify the legal entities»). More importantly:

«The circumstance that the copies of electronic devices may contain documents with no connection to the targeted offences is without incidence on the validity of the operations at this stage of the seizure. It is now about proceeding to a sorting (*tri*) of the IT data copied onto external hard disks from the computers and USB flash drives of the companies and their administrators, issuing a *procès-verbal* of the seizure including an inventory of the relevant documents, and definitively erasing the documents which are irrelevant (*étrangers*) to the open criminal proceedings. The pre-trial chamber of the Court of Appeal notes that the appellants did not contest the validity of the judicial police investigators' mode of operation» [88].

The pre-trial chamber of the Court of Appeal thus validated what is reported to be the standard operating procedure in three steps: making a "working copy" (SNT), sorting and filtering relevant data (SNT), and issuing a new seizure order of the relevant data (investigating judge) [89]. Writing in a personal capacity, an investigating judge has accordingly recommended documenting in the *procès-verbal* ("PV") all steps of making a forensic copy of servers/hard disks, since the seizure of a copy of all data of e.g. a company is more susceptible to give rise to later challenges than a direct extraction of the relevant data [90]. It is however difficult to discern how often in practice a working copy of all data is taken, as opposed to performing filter and extraction on the seizure site [91]. At interview, a member of the SNT remarked that in some cases where data extraction is performed at the place of seizure, time constraints

[88] Ch. c. C., 24 November 2014, n° 860/14.

[89] M. Kraus, *La collecte de preuves informatiques en droit pénal*, in *Pasicrisie Luxembourgeoise*, 2017, No. 2017/3, p. 236.

[90] *Ivi,* p. 231.

[91] In relation to cybercrime, Putz writes that in practice «seizures are generally very broad and cover the entirety of IT equipment. For example, in child pornography cases, if files are found on one device, all devices and equipment found at the suspect's residence are usually seized and consulted. Holiday photographs and private messages are thus in effect copied onto the servers of the police. When drug dealers are arrested, the seizure of all mobile telephones is systematically made. For cybercriminals, the approach is the same»; J.-L. Putz, *Cybercriminalité,* cit., p. 253.

and the terms of the judicial order may lead to potentially valuable data being left behind. This tends to occur where it is necessary to identify which part of data held by a third party company corresponds to the suspect(s), who may use aliases, etc., and it is not feasible to repeatedly revise the terms of the judicial order.

In another set of proceedings, assiduous record-keeping was not enough to ensure the legality of judicial orders to seize data stored in Luxembourg in the course of a complex, tortuous affair entailing accusations of kidnapping and murder in Kazakhstan, letters rogatory issued in relation to spying and duress (*Nötigung)* in Austria, and finally allegations of criminal breaches of data protection legislation in Luxembourg. In relation to the latter, "domestic" proceedings, two judicial orders had been simultaneously executed on a company storing data in Luxembourg on behalf of an Austrian law firm.

One order was annulled on proportionality grounds [92], with the pre-trial chamber of the Court of Appeal eventually concluding, «in view of the enormous quantity of data stored on the seized devices» that the search and seizure constituted a search for as-yet-unknown offences, prohibited by the CPP [93]. The other order concerned not raw data to be seized in the field, but twelve hard disks in the possession of the SNT, containing the results of a *filtrage informatique* which had previously been carried out on data seized pursuant to earlier letters rogatory issued by Austria to Luxembourg. In fact, those initial proceedings had been closed in Luxembourg after the Austrian prosecutor's decision to issue letters rogatory was subsequently annulled by an Austrian court. Upon annulment in Austria, the Luxembourgish investigating judge ordered the release (*mainlevée*) and restitution of all seized data, before immediately seizing it again – this time in relation to fresh allegations made in the meantime in Luxembourg. The pre-trial chamber of the District Court of Luxembourg decided that this background posed no problem with regard to the first order, on the grounds that it targeted

[92] The order sought seizure of two HP servers, a hard disk, and over a hundred cassettes dating back to as early as 2001. It was annulled partly due to its covering data generated at a time when the criminal acts under *instruction* could not possibly have been committed, and annulled entirely due to its covering «the totality of the legal office's IT devices located in Luxembourg without a selection being made between the data relating to the affair (...) and the legal office's other documents unrelated to this affair».

[93] Articles 31(3), 66 and 50, Luxembourg *Code de procédure pénale.*

the same data which the investigating judge could hypothetically have seized in the absence of any Austrian request for mutual legal assistance. The second order, on the other hand, targeted data which «owe their existence» to and had been «confected» on the basis of an act of mutual legal assistance which had since been revoked. Adding that it was not convinced of the usefulness of the data to the discovery of the truth, the chamber annulled the order and recalled an earlier decision establishing that the destruction of IT data across all police systems is an automatic corollary of the restitution of objects which have been seized illegally [94].

There are no specific proportionality rules for digital investigations in the taxation context.

1.8. *Privileged information*

Whether seizures are carried out by the judicial police unassisted (in the urgent *crime flagrant* scenario) or under the supervision of the investigating judge, «all useful measures» must be taken in advance (*préalablement*) in order to ensure the respect of professional secrecy [95] and of the rights of the defence [96]. Lawyers' workplaces and the confidentiality of their communications with clients are in principle inviolable [97]. When any measure *inter alia* of a judicial inquiry is carried out «upon or regarding a lawyer» (*auprès ou à l'égard d'un avocat*), the president of the Bar (the *Bâtonnier*) or his representative must be present. The latter may address his observations concerning the safeguarding of professional secrecy. The seizure act and the search PV must mention, on pain of nullity,

---

[94] Ch. c. C., 18 June 2014, n° 423/14, in *Jurisprudence.* The public prosecutor had argued that the destruction of data which had been illegally copied was a reparative measure of a civil nature, and thus beyond the remit of the pre-trial chamber. The pre-trial chamber of the Court of Appeal disagreed, upheld the challenged decision, and added that the data are to be destroyed on all the devices of the investigating authorities (*autorités poursuivantes*) and that there should be a ban on their use.

[95] Article 458 of the Luxembourg *Code pénal* criminalises any unauthorised breach of professional secrecy, foreseeing sanctions of imprisonment (eight days to six months) and a fine (500 to 5000 euros). It applies to lawyers via Article 35(1) of the Law of 10 August 1991 on the legal profession, Mémorial A N° 58, 27 August 1991.

[96] Articles 33(3) and 65(4), Luxembourg *Code de procédure pénale.*

[97] Article 35(3), Law of 10 August 1991 on the legal profession.

the presence of the *Bâtonnier* or his representative, as well as any observations made by the latter [98]. Furthermore, jurisprudence has considered that the application of the rules of criminal procedure may be influenced by internal regulations (*règlement d'ordre intérieur*) issued by the Bar Council (*Conseil de l'ordre du Barreau de Luxembourg*) [99]. Most importantly for present purposes, a 2013 regulation (since amended) elaborates upon the precise remit of professional secrecy and of lawyers' duties to actively uphold it [100].

All of these provisions received ample application in notorious proceedings before the pre-trial chambers in 2014, which concerned coordinated searches and seizures targeting lawyers and revealed a veritable litany of procedural errors [101]. Insofar as digital investigations are concerned, the sheer disproportionality of the seizure of devices/data executed is extraordinary: whereas just one lawyer was suspected of criminal wrongdoing, seizure was made of all of the electronic files of the legal office – where at least six lawyers worked!

In an admonitory tone, the pre-trial chamber of the District Court of Luxembourg recalled that «the seizure of electronic files cannot accord more freedoms to the seizing authority than physical documents», and remarked that the latter evidence had by contrast been seized in application of precise search criteria. Making direct reference to the emphasis placed by the European Court of Human Rights in *Wieser v. Austria* on the strict observance of procedural rules requiring the compilation of a report at the end of a search along with a list of seized objects, the chamber strongly condemned the PVs of both the investigating judge and the police for not detailing «concretely» how the provisions of Article 66(2) CPP had been respected in light of the reservations expressed by the lawyers during those operations. Again citing analogous reasoning from *Wieser,* the chamber also criticised the execution of multiple acts of

---

[98] *Ibidem*.

[99] See Article 19, Law of August 1991 on the legal profession, cit., and Ch. c. C. n° 316/12, 23 May 2012, in *Jurisprudence.*

[100] See 'Title 7. Professional Secrecy and Confidentiality' in *Règlement Intérieur de l'Ordre des Avocats du Barreau de Luxembourg* (...), Mémorial A N° 39, 6 March 2013.

[101] Ch. c. Lux. (Chambre du conseil, Tribunal d'arrondissement de et à Luxembourg), 2 April 2014, N° 927/14, in Jurisprudence. See further S. MENETREY, *Perquisitions et saisies chez l'avocat*, in *Pasicrisie luxembourgeoise*, 2014, No. 4/2014, p. 796 ff.

search and seizure in several different locations on the same day; in the chamber's words, the representative of the *Bâtonnier* could not «be present everywhere at the same time». In sum, the chamber found nothing in the dossier submitted to it showing fulfilment of the injunction in Article 33(3) CPP to «take (*provoquer*) in advance all useful measures» in order to ensure respect of professional secrecy and of defence rights. Annulment, restitution and destruction of all seized data across police and judicial systems were duly ordered.

Shortly thereafter, in another decision revolving around the seizure of data from a law firm, the pre-trial chamber of the Court of Appeal approved just such «useful measures» [102]. In this case, all parties (the lawyer suspected of criminal wrongdoing, his lawyer, the investigating judge, the *Bâtonnier* and the SNT police officers) agreed in advance in writing that the hard disks from the law firm's computers would first by copied (at the law firm) onto police hard disk drives, and that the latter would be placed in a sealed room (*mis sous scellés*) within the offices of the police. The police would only be able to enter this room in the presence of the *Bâtonnier* (or a representative) and a representative of the law firm in order to proceed, using special software, to the indexation of the copied data and their exploitation by keyword. Should results emerge from the analysis, the documents found would be listed in a PV along with any observations the *Bâtonnier* may wish to make in respect of their relevance to the aims of the judicial inquiry. In this case, the results were first handed to the lawyers under investigation in order for them to verify which data the investigators considered «useful to the discovery of the truth». A meeting was subsequently called at which the lawyers, their counsel, the *Bâtonnier* and a magistrate from the public prosecutor's office were invited to comment on the seizure of those data. The investigating judge then decided which data to seize.

The chamber deemed this procedure to allow maximum preservation of the interests and rights of the parties involved: once the data had been copied the firm could continue using its computers as per usual, the sealed room solution excluded «any clandestine manipulation of the copied data», and the definitive erasure of the irrelevant data – which could be verified by the parties – made it impossible to carry out investigations into activities which were not

[102] Ch. c. C., 11 November 2014, N° 824/14, in *Jurisprudence.*

targeted by the judicial inquiry [103]. The potential of such methods, however, remains open to question on resources grounds. Writing in a personal capacity, a leading investigating judge has thus remarked that in the case at hand, the judicial police had to dedicate an office exclusively to the analysis for several months, with its duration unsurprisingly stretched by the need to assemble all representatives for each entry and session. As such, parsimonious use of such measures by the investigating judge is not only advised but inevitable [104].

1.9. *Chain of custody and data protection*

No soft regulation or checklist of operations for digital seizures were uncovered by desk research or through an interview with two representatives of the SNT, and this observation is borne out in several decisions of the pre-trial chambers of the "instruction courts" detailed throughout this report. Writing in a personal capacity, an investigating judge has stressed the importance of taking precautions in order to ensure data on seized devices are not modified, warning that «although the SNT's specialised investigators know how to react regarding seizure of computers or smartphones, this is not necessarily the case for all police officers who have to carry out searches in the course of their duties» [105]. The judge advises that police officers follow *Electronic evidence – a basic guide for First Responders*, published in 2015 by ENISA, and insists that when examining a switched-on computer on the seizure site, «the investigator must absolutely document the different stages of their intervention» [106].

No legal rules, soft regulations or checklist of operations for digital seizures were detected in the tax field.

In terms of criminal proceedings, typically the officer of the judicial police draws up a report, or the investigating judge will make a PV, translatable as official report or statement, of his operations [107]. Seized data are inventoried in the PV [108], which is

---

[103] The time limits in this case, however, were further challenged by the defence – as discussed in Section 3 below.

[104] M. KRAUS, *La collecte de preuves informatiques en droit pénal*, cit., p. 233.

[105] *Ivi,* p. 229.

[106] *Ibidem*.

[107] Articles 63(4) and 65, Luxembourg *Code de procédure pénale.*

[108] Article 66(2), Luxembourg *Code de procédure pénale*

signed *inter alia* by the concerned person [109]. If that person refuses to sign, this is noted in the PV. A copy of the PV is left with the concerned person. There are no further legal requirements for the contents of a PV, and a standard paper form is used for all types of searches and seizures (*protocole de perquisition et de saisie)* with no distinction made for digital investigations. According to an interview carried out at the SNT, an internal procedure for seizures of data is in place within the police services, but there is no formal "US-style" chain of custody procedure for each step of the digital investigation. Rather, each standardised document is signed by the individuals involved: the report/PV from the scene of the seizure; the request for assistance sent by the investigator to the SNT; the analysis sent back to the investigator; the investigator's follow-up request to the SNT, and so on. This is in many cases an iterative process, as investigators narrow down what they wish to target. As detailed in several places in this report, decisions before the pre-trial chambers of the "instruction courts" have condemned procedural errors and validated certain further precautions to be taken, especially with regard to seizures of data pertaining to legal professionals.

Should personal data be implicated in digital investigations, the keeping of internal records by the judicial police is, as briefly noted at the top of the report, regulated since 2018 by the LED implementation law. In particular, Article 23 of that law imposes a horizontal duty on data controllers to keep a register of all categories of processing activities under their responsibility including *inter alia* the name and contact details of the controller, the purposes of the processing, an indication of the legal basis for the processing operation, and descriptions of the categories of data subject and of the categories of personal data. Data processors (*sous-traitants)* are also subject to less stringent record-keeping requirements. Automated processing systems are subject to specific logging (*journalisation)* requirements in Art. 24 of the implementation law, in the aim of making it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs shall be used solely for verification of the lawfulness of processing, self-

[109] Article 66(5), Luxembourg *Code de procédure pénale.*

monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings [110].

Where Phase Two operations concern personal data, the just-described data protection obligations (record-keeping and logging) apply to the investigating authorities. Otherwise, there is no specific legal duty to write a report for Phase Two *per se*. Nonetheless, according to our interview with the SNT records of processing are systematically kept. This is supported by comments from an investigating judge, who writes that in each dossier in which it is involved, the SNT summarises the results of its research in a report which goes into the criminal case file and is thus available to the investigators, the investigating judge, the defence, the public prosecutor, the pre-trial chambers and the trial courts [111]. There are no rules on how such a report must be compiled, but again according to the SNT interview it is a fairly regular occurrence for judges to question police officers on the methods they have used in their analysis before the pre-trial chamber (see further in Section 4 below). Using the same forensic analysis method as is used abroad «by the majority of experts», writes the judge, ensures that an outside expert may also examine the original seized physical device without its content having been modified by the SNT's analysis [112].

1.10. *Duties and prerogatives of the investigating judge*

Follow-up proceedings [113] in the "useful measures" case described above – concerning seizures carried out at law firm's offices – have led the pre-trial chambers to address two further technical aspects of the proportionality of the "copy, filter, share, seize" process, applied in that case to lawyer-suspects, which fit within Phases One and Two.

Concerning the first "copy" stage (Phase One), the defence argued that the copy made at the law firm had not been sufficiently limited temporally in order to target as precisely as possible the documentation relating to the lawyer-suspect. On this point, the pre-

[110] Art. 24(2), LED Implementation Law.

[111] M. KRAUS, *La collecte de preuves informatiques en droit pénal*, cit., p. 236 f.

[112] *Ibidem*. It has been reported that in practice copies are often made using a dump, allowing for preservation of the state of data at a certain moment in time; hash value calculation will thereafter reveal any subsequent alteration; see J.-L. PUTZ, *Cybercriminalité*, cit., p. 264.

[113] Ch. c. C., 8 July 2015, n° 596/15, in *Jurisprudence.*

trial chamber of the Court of Appeal decided in favour of the investigators: as it had not been demonstrated that the dates of files and folders could not have been manipulated or hidden, a search based on visible dates would risk failure.

Moving on to the subsequent "filter, share, seize" stages of the process (straddling Phases One and Two), having received the results of the police-operated filter the defence complained of differences between the keywords featuring on a list shared with them (pre-filter) and those used in reality by police analysts – leading to an overly-broad analysis akin to a "fishing expedition" and hampering the effective use of the defence of the shared results [114]. The pre-trial chamber of the District Court considered that the defence had had ample opportunity to challenge the use of keywords, either by addressing their observations upon learning which keywords would be applied to the data (which they had in fact done, by email) or by challenging the seizure of data effected using contested keywords, or at least to have observations in that regard taken down, upon formalisation of the seizure [115].

The pre-trial chamber of the District Court declined, however, to specifically address whether the use of "new" keywords could have any impact on the integrity (*régularité*) of the procedure. This issue thus fell to the pre-trial chamber of the Court of Appeal, which referred back to the very role of the investigating judge, who proceeds to all acts of *information* which she judges useful to the discovery of the truth, and thus stated the chamber is «free to use the keywords she judges the most appropriate to the search for relevant documents without being blamed for (*sans qu'il puisse lui être reproché*) the discrepancy between the relatively small volume of documents with a link to the facts in relation to which she is seized and the scale of the documentation that she is called upon to verify during her inquiry».

1.11. *Digital forensic laboratories and storage of seized data*

Our research detected no digital forensic laboratory in

[114] Since the keywords involved at different stages are either not included or are redacted in the text of the decision, it is not possible for the reader to gauge precisely the entire procedure.

[115] Ch. c. Lux., 8 May 2015, N° 1297/15, in *Jurisprudence.*

Luxembourg other than that within the SNT, composed of IT forensic experts who double as police officers, and who carry out all relevant analysis "in-house". It was confirmed at interview with the SNT that no ISO-certified digital forensics laboratory exists in Luxembourg.

Seized data are deposited at the registry (*greffe*) of the competent District Court or with a *gardien de saisie*, pending resolution of the proceedings [116]. There appears to be no limit on how long seized data may be stored at the *greffe*, should no nullity or action for restitution be founded. As noted above, where a nullity is granted by the pre-trial chambers of the instruction courts, the destruction of all data is automatically ordered across all police systems. Otherwise, according to Articles 4 and 7 of the LED implementation law, retention periods for personal data are set by the data controller in light of the goal of the processing, procedural rules must be in place to that end, and those rules must be communicated to data subjects. At interview, members of the SNT stated that a project is underway in order to improve the "follow-up *informatique"* i.e. who performed which part of the chain of custody, and where precisely specific evidence is stored.

1.12. *Cooperation with OLAF*

We close this section with our research findings on OLAF and Luxembourg. For the period 2014-2018, in Luxembourg there were zero detected cases of irregularities in area of Traditional Own Resources ("TOR"), two detected cases of irregularities in areas of European Structural and Investment Funds and Agriculture – but zero investigations closed with recommendations [117]. For the period 2012-2018, Luxembourg saw a total of 5 indictments following OLAF recommendations, compared to 8 dismissed and 5 pending. According to interviews carried out in the course of a previous research project, OLAF usually contacts national authorities at an early stage and transmits the case file to them. National authorities then continue with the investigation, thereby enhancing the admissibility and credibility of evidence. As a result, on-the-spot checks by OLAF are reported to be very rare in Luxembourg [118].

---

[116] Articles 33(7) and 66(6), Luxembourg *Code de procédure pénale.*

[117] The OLAF report 2018, p. 38, p. 41.

[118] K. LIGETI-F. GIUFFRIDA, *Luxembourg*, in F. GIUFFRIDA-K. LIGETI (eds.),

In a case decided in 2015, a defendant complained that the investigating judge's inclusion of an OLAF report in his dossier without carrying out his own investigations breached the judge's duty to conduct investigations *à charge et à décharge* as set out in Article 51 CPP. This contention was rejected by the pre-trial chamber of the Court of Appeal, which concluded that there was no need to repeat activities, and added that OLAF had itself investigated *à charge et à décharge,* so that no violation of the right to a fair trial could be established [119].

2. *Investigating authorities*

Although some stages of digital investigations may map onto both Phase One and Phase Two, in Phase One the process revolves around the judicial police, whether pursuant to a judicial order (in the course of a judicial inquiry), on the authority of the public prosecutor (where competent i.e. in the preliminary investigation scenario; in a *mini-instruction)*, or in the restricted urgent scenario of *crime flagrant.*

Reflecting the strong influence on Luxembourg's criminal justice system of the Napoleonic tradition of separating the functions of *poursuite, instruction* and *jugement*, unless otherwise stated a judicial inquiry is mandatory for crimes, whilst it is optional for felonies (*délits*) – which the public prosecutor handles [120]. The investigating judge may perform, in conformity with the law, any *acte d'information* which she deems useful to discovering the truth. She gathers and verifies, with equal care, the facts and circumstances tending to inculpate or exculpate (*à charge ou à décharge*) the *inculpé* [121]. An investigating judge may not sit on proceedings before the pre-trial chamber in relation to cases which she has instructed [122]. Likewise, investigating judges are prohibited from taking part in the eventual trial [123].

In practice, the judicial police typically executes seizures on behalf of the investigating judge, systematically involving members of its SNT. As detailed in several places above, when large volumes

Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings, 2019, published online at *orbilu.uni.lu/handle/10993/40141*, p. 195 f.

[119] Ch. c. C., 6 January 2015, n° 09/15, in *Jurisprudence.*

[120] Article 49, Luxembourg *Code de procédure pénale*.

[121] Article 51, Luxembourg *Code de procédure pénale.*

[122] Art. 125bis, Luxembourg *Code de procédure pénale*.

[123] Art. 27(2), Luxembourg *Code de procédure pénale.*

of data are seized (given that the visualisation of each file would be painstaking) investigators most often index all available data, before searching within all data using keywords. Upon completion of the search by keywords, the relevant files and data are saved on a police device which the investigating judge may then seize in turn [124].

In the VAT context, although the VAT Administration is inevitably a complex operation whose activities map with great difficulty onto Phase One and Phase Two, most of the relevant functions of Phase One would appear to be centralised within the Administration's Anti-fraud service (*Service anti-fraude*), which is in charge *inter alia* of in-depth inspections in matters of VAT; searching for and detecting all violations/offences (*infractions*) in VAT matters; and the analysis and follow-up of inspections [125]. "Bulletins" and tax fines are emitted by the Administration's Director (or his deputy), who is external to the Anti-fraud service. As mentioned above in Section 1, tax fines can be appealed to the District Court of Luxembourg, sitting in civil matters.

2.1. *Experts and training*

The functions of the judicial police's SNT specialists in criminal proceedings were set out above. All other recourse to "experts" appears to be optional; more precisely, this is decided by the investigating judge during her judicial inquiry. The judge does so by way of a judicial order in which she specifies the information she wishes to obtain from the experts, as well as the questions to which she calls their attention and to which she requests the solution [126]. The *inculpé* may (but without delaying the work of the judge's expert) choose her own expert who is entitled to attend all operations, to address all requests to the experts designated by the judge, and to record his observations on the report of the former in a separate report [127]. Should the judge-ordered expertise be made without the *inculpé* being represented, he has the right to choose an expert who will examine the work of the judge-ordered experts and present observations. Should any of these conditions be flouted, a

[124] M. KRAUS, *La collecte de preuves informatiques en droit pénal*, cit., p. 236.
[125] Article 8, Grand-Ducal Regulation of 10 December 2018.
[126] Article 87(1), Luxembourg *Code de procédure pénale.*
[127] Article 87(3), Luxembourg *Code de procédure pénale.*

ground for nullity is established [128]. The *inculpé,* his advisor and the *partie civile* have the right to request an *expertise* on the facts they indicate, and to ask that the *expertise* ordered by the judge examine those facts. Should the judge refuse, her order must include the reason for the refusal [129].

Although the *expertise* provisions have generated abundant jurisprudence, none of relevance to digital investigations was found. A leading investigating judge, commenting in her personal capacity, has stated that recourse to IT experts is in fact never made (by the public side) in practice due to costs concerns [130]. According to an interview with the SNT, recourse to an IT expert by the *inculpé* or defendant is also very rare. Anecdotally, reference was made to one case entailing an independent expert who withdrew his expert analysis once he became aware of the contents of that carried out by the investigators at the SNT. As noted at several places above, the investigating judge may order any person – except the person who is the subject of the judicial inquiry, who retains the right to remain silent – to assist in giving access to seized systems or to data therein or accessible therefrom, as well as in understanding the protected or encrypted data [131]. This assistance is mandatory, but unlike in Belgium and France [132] no criminal penalty is foreseen for those who do not comply with the judicial order.

No such legal requirements were detected within the applicable tax rules.

There is no register *per se* for such experts, but the website of the Luxembourg Ministry of Justice maintains lists of *experts assermentés,* with a handful self-described as specialising in IT and/or cybercrime [133]. According to an interview with the SNT, these experts put themselves onto the lists, and there are no requirements as to qualifications or certifications.

---

[128] Article 87(7), Luxembourg *Code de procédure pénale.*

[129] Article 88, Luxembourg *Code de procédure pénale.*

[130] M. KRAUS, *La collecte de preuves informatiques en droit pénal*, cit., p. 230. In the cybercrime context, it was reported in 2017 that the SNT had in the past used specialists from CIRCL (Computer Incident Response Center) Luxembourg, from Europol-EC3 or automated tools from private enterprises for the examination of malware – but presumably without a judicial order designating an "expert" in the sense of the CPP; GENVAL Evaluation, cit., at 5.2.2.

[131] Article 66(4), Luxembourg *Code de procédure pénale.*

[132] M. KRAUS, *La collecte de preuves informatiques en droit pénal*, cit., p. 235.

[133] All lists of *experts judiciaires* available at *mj.public.lu/professions/expert_judicaire/Liste_des_Experts/*.

The SNT officers themselves are recruited from outside and trained as police officers, with standard police employment examinations. In 2017 the SNT was cited – in the cybercrime context – as an example to the rest of Europe with regard to its composition, its tasks and its positioning at the international level. In particular, the possibility for "civilian" IT experts to qualify as officers of the judicial police was deemed to enable a fruitful *rapprochement* of skills, which Council of Europe evaluators put forward for development at the European level [134]. There are no specific requirements in terms of training or qualifications for the role, but at interview members of the SNT stated that outside training includes that organised by the International Association of Computer Investigative Specialists (IACIS). Training is refreshed and competence re-assessed periodically. At the time of writing, the IACIS website shows 9 members from Luxembourg. It is worth noting that Luxembourg is not a member of the European Network of Forensic Science Institutes (ENFSI).

It has not been possible to confirm whether the defendant or the subject of the administrative investigation is entitled to check the certificate of independent experts. As noted above, recourse to digital forensics experts would appear to be very rare in practice.

3. *Defence and third-party rights*

There are no specific legal requirements with regard to information on the rights granted to subjects in digital investigations. Nor are there specific legal requirements with regard to aspects of the report of the procedure of digital investigations which must be disclosed to the subject, or any procedural right to gather evidence conferred on subjects in Luxembourg law. The underlying reason for the latter is the central role assigned in inquisitorial systems to the investigating judge [135], who has a statutory duty to search for the truth using powers to gather both inculpatory and exculpatory evidence. The accused is, however, generally free to carry out any act that may boost his defence – except coercive measures – and (as discussed in Section 4 below) there is in principle no limitation on evidence which may be admitted at trial.

---

[134] GENVAL Evaluation (2017), cit., p. 32.
[135] V. COVOLO, *Report on Luxembourg*, cit., at V.1.

At the pre-trial stage, the subject may also request that the investigating judge take certain measures, including the appointment of an expert (as just discussed in Section 2). Since 2018, a third party with a legitimate personal interest can do the same. This amendment was deemed necessary in order to redress an imbalance revealed by criminal proceedings in which the *expertise* employed by the *inculpé* had led to a third party being suspected of criminal wrongdoing and then, in turn, being *inculpé*. Whereas third parties already had the power (under Article 126 of the CPP) to request the nullity of an *expertise* concerning them, the reform extended the third party's right to make a request to the investigating judge to have their own expert engaged [136].

In conformity with the distinction between the functions of *poursuite, instruction* and *jugement*, as a general rule the public prosecutor's preliminary investigation may only take non-coercive measures [137]. As such, where consent is not given by the subject of digital investigations, a judicial inquiry is necessary (with the limited exception of the *mini-instruction*) in order to execute a seizure. In practice, there seem to be cases where consent is given to either copy data (e.g. from a social media account or email account) or to access open connections "in the cloud" discovered during a search [138]. If such consent is not given, a judicial order is sought. No case law was found which addresses this matter [139].

Although full access to the case file is systematically available to the defence, as noted in several sections above there are no digital investigation-specific guarantees with regard to disclosure. Given the lack of relevant statistics and the relative dearth of case law (in turn partly due to the centrality of the investigating judge and of pre-trial hearings, which are not public) in what is a small-sized criminal justice system, further targeted research in the years to come would

---

[136] Projet de loi n° 7720, Exposé des motifs, p. 12.

[137] See G. Vogel, *Lexique de procédure pénale de droit luxembourgeois,* 3rd ed., Larcier, Brussels, 2009, p. 60.

[138] Genval Evaluation, cit., at 5.2.2.

[139] See further M. Kraus, *La collecte de preuves informatiques en droit pénal*, cit., who writes: «for effectiveness reasons, this solution has already been used in the course of certain searches where data are stored remotely and useful for the discovery of the truth were directly accessible without requiring supplementary acts. In the absence of jurisprudence in Luxembourg in this matter, it would be worth expressly providing for this solution in the CPP»; p. 234. Similarly, advocating the adoption of a legislative solution along German or French lines, see J.-L. Putz, *Cybercriminalité,* cit., p. 249-250.

be required in order to make informed observations as to the critical issues concerning the disclosure of digital data, and to shed light for instance on the "dark figure" of defendants who are not accessing (or even considering accessing) independent digital forensics experts in the course of their defence. The key legal arena for the defence would seem to be the pre-trial chambers, where it can claim a nullity on both statutory and substantive grounds, such as where flawed disclosure of evidence imperils the right to a fair trial enshrined in Article 6 of the ECHR. Assessment by the chambers is performed on a case-by-case basis, in a grey area lacking tailored procedural rules for digital investigations, which impedes the drawing of general conclusions with regard to the effectiveness of such remedies.

As seen above in Section 2, when data are seized in the course of digital investigations, they may not be deleted from the subject's device(s) unless a copy is first made [140]. The CPP limits deletion to data whose possession or use is illegal or dangerous for the security of persons or of goods; in practice, this tends to takes place in order to block the commission of further offences involving the spread of malware, or the sharing of child pornography [141]. Besides its use as evidence, preserving a copy of the deleted data is also required in case its restitution is ordered (should the erasure decision be annulled by the pre-trial chamber or the trial court, or should the proceedings end in a dismissal (*non-lieu)* or acquittal) [142]. Article 68(1) of the CPP enables third parties to request restitution, whilst under Article 67 the investigating judge may order on her own motion and at any moment the total or partial release (*mainlevée*) of seized data. At interview, a member of the SNT stated that this power is used regularly, where data are not of an illegal nature, in particular to relieve the burden on small businesses which would struggle to continue operating without access to their main devices and/or data.

In principle, digital investigations carried out by the defendant have evidentiary value; since Luxembourg uses a "free proof" system, any type of evidence is *a priori* admissible before the criminal courts (see further Section 4 immediately below). It is however essential that evidence be useful, "loyally" obtained, and subject to the adversarial principle (*contradictoire*). For example,

[140] Articles 33(5) and 66(3), Luxembourg *Code de procédure pénale.*
[141] M. BRAUN, *La ratification de la Convention de Budapest*, cit., p. 132.
[142] *Ibidem*.

unilateral expert reports are admissible so long as the parties have the opportunity to freely discuss them [143].

4. *Admissibility at trial*

There are no specific conditions or constraints in Luxembourg law regarding the admissibility of digital evidence in criminal proceedings [144]. Furthermore, the fundamental principle of free assessment of evidence by the Luxembourgish trial judge (*la liberté de la preuve*) means that any type of evidence is *a priori* admissible before the criminal courts [145].

Provisions in punitive administrative law are general. Any evidence may be led so long as the adversarial principle (*contradictoire)* is respected in relation to each piece of evidence [146]. Evidence may be brought by any means (except oath) in tax proceedings [147]. With regard to VAT, the VAT Administration is «authorised to prove according to the rules and by all means of common law, except oaths, and, *inter alia,* the reports of its agents, any breach of the present law or the regulations executing it, as well as any fact at all which establishes or contributes to establishing the eligibility of the tax or of a fine. The breaches and facts referred to may also be observed (*constatés*) by means of reports addressed by officers of the judicial police, customs and the *force publique* called upon to collaborate on tax inspections. Reports are presumed to be true until proved otherwise» [148].

Returning to criminal proceedings, in the judicial inquiry context illegally or improperly obtained evidence can be excluded by the pre-trial chambers (of the "instruction courts") on the basis of Article 126 of the CPP. In the preliminary investigation scenario, since there is no judicial inquiry stage, the admissibility of evidence is resolved before the eventual trial court – but before any review on the merits, pursuant

[143] Ch. c. C., 6 December 2013, N° 699/13, in *Jurisprudence.*

[144] Confirmed in Genval Evaluation, cit., p. 51: «There are no specific admissibility conditions for electronic evidence».

[145] V. Bolard, *Preuve et vérité* (trad. "Evidence and truth")*,* in *Annales du droit luxembourgeois*, vol. 23 (2013), p. 39, p. 75.

[146] Articles 14, 30 and 51, Law of 21 June 1999 on proceedings before administrative courts, Mémorial N° 98.

[147] Article 59.

[148] Article 68, VAT Law.

to Art. 48-2(3) of the CPP [149]. The goal of the legislator is clearly to have all admissibility issues adjudicated as early as possible – and ideally before trial. To that end, should an *inculpé* fail to trigger a nullity before the pre-trial chamber or should the chamber reject such a request, the trial court has no power to apply nullities during the proceedings referred to it (*purge des nullités*) [150]. Nullities which can be engaged before the pre-trial chambers may be formal (foreseen in a statutory provision) or substantive (developed in jurisprudence in order to sanction violations of substantive procedural requirements – in particular, breaches of defence rights). Since 2012, the jurisprudence considers that a request for nullity can be based on alleged violations of the right to a fair trial enshrined in Article 6 of the ECHR [151].

In 2007, a landmark judgment of the *Cour de Cassation* established the rule that the trial courts may discard evidence that has been unlawfully obtained if either (i) the non-respect of certain formal requirements is sanctioned by nullity; (ii) the irregularity committed has tainted the credibility of the evidence; or (iii) use of the evidence is contrary to the defendant's right to a fair trial [152]. It is "nonetheless" for the judge to evaluate the admissibility of illegally-obtained evidence taking into account the elements of the case considered as a whole, including the manner in which evidence has been obtained and the circumstances of the illegality committed – in other words, even if none of these three alternative criteria is satisfied, evidence may still be discarded should the *légalité* of the administration of evidence not be ensured overall. In this connection, the Court of Appeal has held that the adversarial discussion of evidence at trial does not suffice to repair irregularities in the gathering of evidence [153].

On occasion, illegally-obtained digital evidence has indeed been excluded at the trial stage following application of this test. This

---

[149] The same rule applies to acts taken in the course of a *mini-instruction;* Article 24-2(3), Luxembourg *Code de procédure pénale.*

[150] V. COVOLO, *Luxembourg*, cit., p. 365 f.

[151] Ch. c. C., 16 May 2012, n° 301/12, in *Jurisprudence.*

[152] Cass. (*Cour de cassation*)*,* 22 November 2007, n° 57/2007, in *Jurisprudence.* Noting the strength of the Court's position in favour of the inadmissibility of illegally-obtained evidence compared to its counterparts in Belgium and in France, see M. MARTY, *La légalité de la preuve dans l'espace pénal européen*, Larcier, Brussels, 2016, p. 274-313.

[153] C.A. (*Cour d'Appel),* 26 February 2008, n° 106/08, in *Jurisprudence*.

was notably the outcome when the public prosecutor, alleging theft by a cleaner of lunch vouchers and gift vouchers from a bank, attempted to rely on CCTV footage of vouchers being spent at a supermarket [154]. The CCTV system, however, had not been authorised by the national data protection authority (CNPD) – which constituted a (criminal) *délit* on the part of the supermarket. The public prosecutor's argument that the gravity of the offence by far outweighed that of the illegality committed in obtaining the CCTV footage was rejected by the District Court of Luxembourg, which decided that the violation of legal rules designed to protect the fundamental rights of individuals (in this instance the right to a private life) was clearly more serious than a banal property offence [155]. The Court emphasised that the duty of loyalty in the administration of evidence incumbent upon the public prosecutor must be considered to be the essence of a fair trial, added that other evidence could have been obtained legally by opening a judicial inquiry, and threw out the evidence.

In the main, however, most such issues in the digital investigations context appear to be settled at the pre-trial stage upon completion of the judicial inquiry. When the pre-trial chamber of the District Court is thus seized by a request for annulment pursuant to Article 126 of the CPP, the jurisprudence states that the only task of the former is to weigh up whether the investigating judge has (i) failed to fulfil a duty imposed upon her on pain of nullity by the law or (ii) acted in violation of the elementary rights of one of the parties in such a way as to produce real and important damage (*lésion*) of the essential rights of the parties [156].

In a 2015 ruling, the pre-trial chamber of the District Court of Luxembourg thus explicitly recognised that due to the absence of any specific legal provisions in Luxembourg governing seizures of computer data, the instruction courts are to evaluate the conformity of each challenged seizure, case-by-case, with regard to both their goal (*objet*) and their implementation (*mise en œvre*), with the general framework set by the CPP vis-à-vis seizures and with the

---

[154] T. A. Lux., 2 July 2014, n° 1872/2014, in *Jurisprudence.*

[155] See further E. Fronczak, *La protection de la vie privée, de l'image et de la correspondance du salarié. Perspectives luxembourgeoise et européennes*, in *Journal des tribunaux Luxembourg*, 2018, i. 1, p. 8 ff.

[156] Ch. c. Lux., 16 February 2012, n° 551/12, in *Jurisprudence*; Ch. c. Lux., 2 April 2014, n° 927/14, in *Jurisprudence*; Ch. c. C., 28 May 2019, n° 494/19, in *Jurisprudence*.

principles developed by the ECtHR in application of the Convention [157].

There are no specific rules concerning the review of admissibility decisions in either court or non-court administrative punitive proceedings. In the case of VAT, fines are subject to *réclamation* i.e. a request that the Administration reconsider its decision. That decision may be challenged before the civil chamber of the District Court of Luxembourg [158].

4.1. *Burden of proof*

A fortiori given its monist tradition the presumption of innocence, enshrined in Article 6(2) and developed through Strasbourg jurisprudence emphasising the burden of proof resting on the accusation, is of central importance to the criminal justice process in Luxembourg [159]. The right to be heard and to give evidence is inherent to the adversarial nature of hearings at the trial stage for felonies and crimes, with a raft of protections set into the CPP and in case law, such as the right of reply *(droit de réplique)*, in effect the right to speak last in order to effectively challenge arguments put forward by the public prosecutor [160].

In the context of misdemeanours (*contraventions)*, which are judged by either the lower-level police courts or the correctional chambers of the district courts, reports by judicial police officers are presumed true until it is proven that the officer falsified the report [161]. No such rule applies, however, where felonies (*délits*) are adjudicated by the correctional chambers of the district courts, or where crimes are adjudicated by the criminal chambers of the district courts. Furthermore, there are no specific rules concerning the chain of evidence. At interview, members of the SNT remarked that in practice judges often ask how certain results were obtained or conclusions were reached in the course of digital investigations.

---

[157] Ch. c. Lux., 8 May 2015, n° 1297/15, in *Jurisprudence,* p. 7.

[158] Article 79, Law of 12 February 1979 on VAT.

[159] See e.g. Cass., 28 April 2016, n° 17/2016, in *Jurisprudence,* p. 25.

[160] Articles 190-1(3) and 222, Luxembourg *Code de procédure pénale.*

[161] Articles 154 and 189, Luxembourg *Code de procédure pénale.* Reports by other agents (e.g. OLAF agents) are also admissible, but their content may be denied simply by proving that facts stated therein are not true; see M. PETSCHKO-M. SCHILTZ-S. TOSZA, *Luxembourg*, cit., p. 467.

Although it was unclear in what degree this remark referred to the pre-trial or the trial stage, for that reason where possible the SNT use open source software, so that steps taken may be explained to the judge(s) in detail, and potentially contested by the defence.

In tax proceedings before the administrative court, the task of proving facts triggering the fiscal obligation "belongs" to the tax administration, whilst facts freeing the taxpayer from the fiscal obligation or lowering it must be proved by the taxpayer. The burden of proving the regularity of the tax procedure also "belongs" to the administration [162]. There are no specific rules for digital investigations.

4.2. *Administrative-criminal crossover*

In light of the "free proof" system in Luxembourg, information gathered by any administrative authority may be admissible as evidence in criminal proceedings. Nonetheless, as the general principles apply, evidence must be useful, collected in a loyal manner, and debated adversarially in order to be admitted [163]. In this regard, it is worth noting that the VAT Administration is bound to transmit information which may be used in criminal proceedings to the judicial authorities [164]. Additionally, any authority, public officer or civil servant etc. which/who becomes aware in the course of its/their duties of facts which are liable to constitute a crime or a felony, must inform the public prosecutor [165].

A relevant example of the stringent approach taken by the Luxembourg courts in this regard emerged from proceedings before the correctional chamber of the district court in which the public prosecutor attempted to rely on screenshots (taken on a mobile telephone) which had first been obtained by the customs authority in the course of an inspection [166]. First, the court made a literal reading of the above-cited CPP provision binding the customs agents to inform the public prosecutor of their suspicions of criminal

---

[162] Article 59, Law of 21 June 1999 on administrative proceedings, cit.

[163] K. Ligeti-F. Giuffrida, *Luxembourg,* cit., p. 194.

[164] Article 16(1), Law of 19 December 2008 on cooperation between tax administrations, Mémorial A N° 206.

[165] Article 23(2), Luxembourg *Code de procédure pénale.*

[166] Corr. (*Chambre correctionnelle*), T. A. Lux., 20 December 2017, 493/17 X, in *Jurisprudence*.

wrongdoing, noting that whereas the Code required agents to transmit all information (*renseignements),* reports (*procès-verbaux)* and related acts (notwithstanding any rule of confidentiality or professional secrecy), it did not extend to the obtaining of evidence*,* which is governed exclusively by the framework of the CPP. Since the public prosecutor had not executed a seizure in accordance with those rules, the evidence was obtained illegally. With that established, the court then applied the strict interpretation of the legality of the administration of evidence established in the 2007 Court of Cassation judgment mentioned above, in order to conclude that the illegally-obtained screenshots violated the right to a fair trial and had to be excluded. The other aspects of the customs agents' report, it having been transferred lawfully, were not excluded.

Lastly, no case law was found touching on any critical issue deriving from the proprietary nature of software used to perform digital investigation, or to open/access digital data. As stated above in various places, in Luxembourg almost all digital investigations (reportedly with the notable exception of decryption operations) are carried out "in-house" by the SNT. As far as possible, SNT agents use open source tools.

5. *Concluding remarks*

By and large, in Luxembourg the standard, technologically-neutral legal rules are applied to digital investigations in both the criminal and administrative punitive contexts. In the few places where the – criminal – legal framework has been adapted to the specificities of electronic data and digital evidence, the impetus to do so has come from a need to keep pace with developments either in neighbouring jurisdictions (the response to the terrorist threat in 2018), or at the regional level (implementation of the Budapest Convention in 2014; implementation of the Law Enforcement Directive in 2018) rather than domestic initiatives. Whereas the seizure of electronic data was reportedly already being carried out on the basis of general provisions in the *Code de procédure pénale* (CPP) – despite their clear emphasis on physical objects – the Budapest reform added a measure of legal certainty to the process of seizing digital evidence without tackling the questions of ensuring its authenticity and integrity.

The CPP provisions set out in this report also confirm the centrality of the investigating judge in the management of criminal proceedings entailing digital forensics and of the judicial police in

executing her orders. Whereas the sub-division of powers and duties between those two actors and the public prosecutor is clearly established, the legal framework has minimal interaction with the concrete digital forensics steps taken by investigators on the ground. Indeed beyond the CPP, no rules, soft regulations or checklists of operations are officially prescribed for digital forensics operations – although there is systematic involvement in digital seizures of a specialised "new technologies" police support unit who benefit from outside training. Moreover, in practice it would seem that notwithstanding the absence of a specific legal requirement to do so, investigating judges – who are independent and impartial by design – regularly scrutinise the workings of digital forensics in the course of their judicial inquiries, and through the adversarial dynamics of proceedings before the pre-trial chambers, accepted and censured practices for digital seizures have gradually been distinguished – especially in cases where lawyers are the targets of investigations.

Gauging the potential effects of this legal grey area on the defence is no simple task, not only due to the double-edged role of the investigating judge and the (current) dearth of jurisprudence in what is a small jurisdiction. In particular, further targeted research in the years to come would be required in order to throw light on the "dark figure" of defendants who are not accessing (or even considering accessing) independent digital forensics experts in the course of their defence. The key legal arena for the defence would seem again to be the pre-trial chambers, operating on a case-by-case basis, where it can claim a nullity on both statutory and substantive grounds, such as where the flawed disclosure of evidence imperils the right to a fair trial enshrined in Article 6 of the ECHR. On the one hand, in terms of admissibility Luxembourg combines a free proof system tempered by a strongly-protective approach in the jurisprudence toward illegally-obtained evidence. On the other, and although full access to the case file is systematically granted to the defence, digital forensics-specific guarantees with regard to disclosure are still missing. The introduction of more detailed legal rules on digital forensics would meet a system which provides ample opportunities to examine levels of compliance with them.

Lorena Bachmaier Winter

THE HANDLING OF DIGITAL EVIDENCE IN SPAIN

1. *Introduction*

We live in an increasingly digitalised world where the information is mainly stored in computers and the communications take place mostly in the digital environment. Thus it is not surprising that digital evidence has gained increasing relevance in all types of judicial proceedings and plays a major role as evidence in cybercrime as well as in all other types of crimes [1]. As it happened

[1] See generally J.C. Ortiz Pradillo, *Problemas procesales de la ciberdelincuencia*, Colex, Madrid, 2013.

with paper documents in the past, the rules to ensure the authenticity and integrity of the electronic data for evidentiary purposes should be, if not the same, very similar regardless if it is obtained to be used as evidence in a civil, administrative or criminal procedure. However, there is no unified legal framework, and thus identifying which standards apply to each of the proceedings, is not clear.

Questions arise also when it comes to the transfer of evidence obtained within an administrative investigation to the criminal procedure, because it is unclear whether the same forensic standards apply in both. Problematic is also to define which rules should apply to the transnational digital evidence, as there are not uniform standards valid at the European level. The following paper aims to identify the legal framework and practice on digital evidence and forensics in Spain, with the focus on criminal proceedings. However as many of the investigations on fraud against the financial interests of the European Union are initiated by OLAF, it is relevant also to determine to what extent the rules applicable to digital investigations and forensics provided in the administrative sanctioning proceedings that qualify as "criminal in nature" are under the case-law of the European Court of Human Rights differ from those provided for the criminal procedure.

For understanding the Spanish context, and the reasons why this study will focus mainly on the rules and practice of criminal investigations, some basic information on the scope and principles of the administrative sanctioning proceedings appear to be necessary.

2. *Some preliminary notions on the applicable legal framework and standards on digital forensics*

The principle of legality recognised in Article 25.1 of the Spanish Constitution (SC) is applicable to administrative sanctions in the same way as for criminal sanctions: «No one may be convicted or sentenced for any act or omission which at the time it was committed did not constitute a felony, misdemeanour or *administrative offence* according to the law in force at that time». Thus most principles and safeguards provided with regard to criminal sanctions are applicable also to the administrative sanctioning proceedings. Those rights can be made effective before the courts through the judicial review of administrative decisions (*proceso contencioso-administrativo*). Articles 77 of Law 39/2015, of 1st October, on the *Procedimiento Administrativo Común de las Administraciones Públicas* (Common Administrative Procedure of Public Administrations), last amended by RDL 14/2019, of 31 October

2019, provides for the rules on means of proof and time to present evidence. In its paragraph 1 it reads: «1. The relevant facts for the decision of a procedure may be accredited by any means of proof admissible in Law, whose assessment will be carried out in accordance with the criteria established in the applicable rules of the Civil Procedure Code» (*Ley de Enjuiciamiento Civil* 1/2000, LEC).

Therefore the applicable rules on digital evidence in administrative sanctioning proceedings are basically the ones provided for expert opinions in civil proceedings under Articles 335-352 LEC. No precise rules on digital evidence are contained in the LEC, although Articles 382 to 384 LEC mention the possibility to present evidence through instruments that reproduce images, words or sounds or stored data (comprising therefore computer files and thus digital evidence)[2]. However, with regard to the digital evidence it is only stated that the parties can present expert evidence on the authenticity and integrity of such means of evidence (Article 382.2 LEC), but there are no further rules specific to this IT expertise.

In practice, digital evidence will be presented and assessed as any other documentary evidence supported by IT expert evidence and usually by way of the witness expert report. No specific rules for this expert evidence are legally provided, although for being considered reliable and thus, to be given full evidentiary value, the protocol to be followed in the collection, acquisition, transportation, analysis, storage and presentation, will be essentially the same as the one applicable to those activities carried out within a criminal investigation[3]. The Public Administration will usually have the relevant data, and they also have the powers to request from the citizens those documents that are needed to fulfill their inspection duties. Nevertheless in cases where digital data stored in a computer are needed for evidentiary purposes, the rules applicable are the ones provided under the LEC although the protocol to be followed will usually be the same as for criminal investigations. Indeed a more precise legislative framework would be necessary, as there is hardly any differentation between evidence

[2] On the IT expert evidence in civil proceedings see S. Puig Faura, *La prueba pericial informática,* La Ley-Wolters Kluwer, Madrid, 2015*,* p. 285 ff.

[3] See generally, L.E. Arellano González and M.E. Darahuge, *Manual de Informática Forense*, Errepar, 2019, p. 47 ff.; J. Delgado Martín, *Investigación tecnológica y prueba digital en todas las jurisdicciones*, La Ley-Wolters Kluwer, Madrid 2016, p. 52 ff.

collected for sanctioning purposes and evidence collected in other administrative proceedings.

Our research confirmed that private digital investigations (for companies, aimed at gathering evidence for labour matter proceedings [4], or for internal investigations within the obligations set out in CCL compliance programmes, etc.), in practice also follow the same protocols, guidelines and standards in the whole digital evidence procedure than the law enforcement agents (LEA) in the criminal investigation [5].

Standards for ensuring the authenticity and integrity of the digital data contained in computers are essentially the same and when it comes to the technical devices, in general private forensic companies use also the same devices as the LEA, mostly based on Israeli technology or imported from Israel companies [6]. Conditions for the legality and validity of the digital evidence are equivalent. In this context it has to be recalled that the Code of Civil Procedure works as general subsidiary law for the rest of the procedural codes, and therefore it is also subsidiarily applicable to the criminal proceedings where there is no specific rule or there is a legal lacuna [7].

When it comes to digital evidence the main differences are (in

---

[4] Information provided by the IT forensic unit of one of the big international auditing and forensics companies.

[5] Reference to the law enforcement agents (LEA) includes both institutions *Policía Nacional* (PN) and *Guardia Civil* (GC). The structure and functions of the law enforcement authorities in Spain (mainly National Police and Guardia Civil) are regulated in Organic Law 2/1986, of 13 March, last modified 29 July 2015 (*Ley Orgánica Fuerzas y Cuerpos de Seguridad del Estado*). When listing the functions, the law mentions both prevention and investigation, without differentiating which authorities or units will carry out preventive functions and which ones will carry out the investigation. Both institutions have competences in criminal investigations and have their own IT forensics units. Although the distribution of their competences is mainly based on geographical criteria, there are also competences divided on the basis of subject-matter. There are also areas, where they have shared competences in criminal investigations, and both of the institutions have their own specialised units. As all the institutional structure is not relevant for the present analysis on digital evidence and digital forensics, it will not be further described.

[6] This information is important as we were unable to get the information on what type of devices LEA IT units use. Despite the different times and different members of the National Police and Guardia Civil contacted, the IT units were reluctant to provide information on the technology they are using for the acquisition and analysis of the digital data.

[7] Article 4 LEC, Supplementary application of the Civil Procedure Code: «In the absence of provisions in the laws that regulate criminal, administrative, labour and military proceedings, the provisions of this Code shall apply to all of them».

addition obviously to the scope of the investigative powers, and standards of proof, etc.): 1) the mirroring or cloning of the computer in private investigations will be done in the presence of a notary, for ensuring the integrity and authenticity of the digital data, while in the criminal investigation, the role of the notary is carried out by the *Letrado de la Administración de Justicia*. Different from other legal systems, this civil servant has the duty to attest the judicial acts. Recently it has enhanced its competences becoming the judicial office manager, but the main duty and responsibility of this officer – with a similar professional education and selection process as a judge – is to act as judicial notary [8]; 2) Expert evidence in the criminal proceedings is provided by official institutions, while in civil proceedings, where the evidence is mainly party driven (Article 216 and 282 LEC), the parties will hire the experts they consider reliable, as the court has limited powers to appoint ex-officio expert witness [9]. The IT experts are integrated within the specialised units of *Policía Nacional* and *Guardia Civil,* while this is not the case in private investigations nor in administrative sanctioning proceedings. After these clarifications, the following paragraphs will mainly focus on criminal proceedings.

3. *Digital investigations: the national framework*

3.1. *The applicable standards in digital forensic procedures*

The Spanish Criminal Procedure Code does not contain precise rules on digital forensic procedures [10], nor does the Civil Procedure Code, so it can be said that there is no specific regulation at the statutory level. However, the courts have developed clear

[8] In this study the expression "judicial notary" will be used to identify the *Letrado de la Administración de Justicia*, even if his/her functions are broader than those of attesting the judicial acts.

[9] On the problems that this regulation causes with regard to the digital evidence, see S. Puig Faura, cit., p. 308-312.

[10] As of 25 November 2020 a new draft law on amending the Spanish Criminal Procedure Code has been adopted by the Ministry of Justice. This draft includes new rules on access to data, data mining and targeted searches. Moreover, the pre-trial investigative phase will be directed by the public prosecutor, and not anymore by the investigating judge. As this draft law is only a preliminary text, subject to amendmnts in the parliamentary process, it has been decided not to refer to it in this text. The general rules on digital forensics and expert evidence should remain as reflected here.

requirements to be fulfilled with regard to the authenticity and integrity of the evidence, as well as regarding the standards to be complied with to ensure the chain of custody [11]. Therefore, despite the lack of an explicit legal regulation, it can be affirmed that there are precise standards on the legality and validity of evidence, also with regard to digital evidence. In addition there are a number of standards and best practices codes, that set the rules on how to handle digital evidence and all the precise steps to be followed in each stage during digital investigations by the LEA [12]. The standards applied by *Policía Nacional* and *Guardia Civil* are:

1) Best Practice Manual for the Forensic Examination of Digital Technology (ENFSI, 2015);

2) ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence;

3) UNE standards [13], which are certified by AENOR (*Asociación Española de Normalización y Certificación*):

UNE 71506 Methodology for forensic analysis of electronic evidence (July 2013) [14].

UNE 71505-1 Information Technology (IT). Electronic Evidence Handling System (SGEE). Part 1: Vocabulary and general principles.

UNE 71505-2 Information Technology (IT). Electronic Evidence Handling System (SGEE). Part 2: Good practices in the management of electronic evidence.

---

[11] On the requirements for ensuring the authenticity of the evidence, see e.g. Supreme Court (Criminal Chamber), 6 April 2016, n. 277; Supreme Court (Criminal Chamber), 18 July 2014, n. 587/2014; Supreme Court (Criminal Chamber), 22 October 2013, n. 773/2013.

[12] This information was confirmed by the relevant LEA units during a meeting organised to gather practical information in June 2019 with 8 members of the *Policía Nacional* and *Guardia Civil*, mainly from the International Cooperation Unit. A separate meeting was organised with the Unit on Interception of Telecommunications of *Guardia Civil*. I want to express my gratitude to the very professional members of both institutions who provided relevant information for this study and in particular to the Comisaria Principal Alicia Malo, Head of the Unit of International Cooperation of the Policía Nacional.

[13] UNE is the acronym for 'Una Norma Española'. The Spanish title of these standards has been translated into English for clarity reasons.

[14] This standard has been prepared by the technical committee AEN/CTN 71 Information technology whose Secretariat is AMETIC: *Asociación Multisectorial de Empresas de Tecnologías de la Información, Comunicaciones y Electrónica*. AMETIC was founded in 1984 and represents approximately 3.000 companies of the information and communications technologies (ICT) in Spain.

UNE 71505-3 Information Technology (IT). Electronic Evidence Handling System (SGEE). Part 3: Formats and technical mechanisms.

UNE 197001:2011 General criteria for the preparation of reports and expert opinions. CEN/Guide 14 Common policy guidance for addressing standardization on qualification of professions and personnel.

4) UNE 197010 General criteria for the preparation of reports and expert opinions on Information Technology and Communications (ICT) of 25 March 2015, which refer to the UNE standards above and also to the ISO/IEC 27037: 2012 Guidelines for the identification, collection, acquisition and preservation of digital evidence. In complying with these standards, the Spanish authorities are in comlpiance with the standards set out in the Council of Europe Electronic Evidece Guide. A Basic Guide for Police Officers, Prosecutors and Judges [15].

3.2. *The proportionality principle in digital investigations*

The principle of proportionality is not expressly mentioned in the Spanish Constitution of 1978, but Art. 106(1) recognises it as a guiding principle of administrative law by stating: «The Courts control the power to issue regulations and to ensure that the rule of law prevails in administrative action, as well as to ensure that the latter is subordinated to the ends which justify it» [16]. Before the Organic Law 13/2015, of 5 October amending the Criminal Procedure Code (*Ley de Enjuiciamiento Criminal*, LECRIM), the access to digital data stored in computers was regulated by analogy to the rules on search and seizure and on telephone tapping. The constitutional principles of proportionality and necessity have been steadily applied when assessing the limits of the interferences on the right to privacy and the right to the secrecy of communications within criminal investigations [17].

---

[15] This guide has been published in June 2020 and is accessible at: https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4.

[16] On the case law about the principle of proportionality of the Spanish Cosntitutional Court, see generally, e.g., M. González Beilfuss, *El principio de proporcionalidad en la jurisprudencia del Tribunal Constitucional,* Aranzadi, Cizur Menor, 2003; C. Bernal Pulido, *El principio de proporcionalidad y los derechos fundamentales*, CEPC, Madrid, 2003.

[17] See, e.g. C. Zoco Zabala, *Nuevas tecnologías y control de las comunicaciones*, Civitas, Madrid 2015, p. 102 ff.

Following the case law of the Spanish Constitutional Court the right to privacy *(intimidad)* recognised under Article 18.1 SC is linked to the sphere of life a person wants to preserve from prying eyes, that area the individual wants to keep hidden from others because it belongs to her private sphere [18]. This right is closely linked to human dignity and the right to the free human personal development (Article 10.1 SC). Thus the right to an inaccessible core of privacy is granted even to those persons who are most exposed to public view [19]. The right to privacy, according to the constitutional provision, is recognised not only to the individual, but also to the family [20]. In addition, Article 18.3 SC expressly provides for the protection of the privacy of communications, as follows: «Secrecy of communications is guaranteed, particularly of postal, telegraph and telephone communications, except in the event of a court order to the contrary» [21].

Regarding the access to data and the interception of communications, the proportionality principle has to be respected. In the very relevant judgment of the *Tribunal Constitucional* STC n. 55/1996, of 28 March 1996 the Constitutional Court – although focused on the proportionality principle of the criminal sanction with regard to the criminal act committed – stated the principle that every restriction of the exercise of a fundamental right «adopted in protection of another fundamental right must be balancing both rights and has to be proportional to the content and purpose of both rights» [22]. The Court also held that «the principle of proportionality in our constitutional system is not an autonomous constitutional principle which can be invoked separately from other constitutional rights» [23].

Following the European Court of Human Rights' approach [24], the

---

[18] See Judgment of the Tribunal Constitucional (STC), 29 September 1997, n. 151/1997.

[19] STC, 15 July 1999, n. 134/1999.

[20] See e.g., STC, 2 December 1988, n. 231/1988; STC, 17 October 1991, n. 197/1991.

[21] See J.J. FÉRNÁNDEZ RODRÍGUEZ, *Los datos de tráfico de comunicaciones: en búsqueda de un adecuado régimen jurídico que elimine el riesgo de control permanente, REDC*, 108 (sept.-dic.) 2016, p. 93-122, at 101, on the extension of the protection of the secrecy of communications under art. 18.3 SC also to the internet traffic data or metadata.

[22] Quoting STC, 8 June 1992, 85/1992.

[23] *Fundamento Jurídico* n. 7.

[24] See, among others, ECtHR, Kopp v. Switzerland, 25 March 1998; ECtHR,

Spanish Constitutional Court applies the proportionality check comprised of: control of the adequacy or appropriateness of the measure under consideration (means-end relationship)[25]; examination of the need for it (absence of a less intrusive alternative measure); and the strict proportionality control (the conflicting interests involved which are to be weighed to check if the advantages outweigh or at least offset the disadvantages)[26]. Regarding the interception of communications (telephone), the Constitutional Court in its decision 49/1999, of 5 April 1999 stated that the principle of proportionality requires that both the legal provisions and the practice on telephone interceptions are limited to a constitutionally legitimate aim[27] and such interference will only be justified if the restrictive measure is strictly necessary to achieve that aim and such sacrifice is proportionate.

Those principles have been set out in the legal provisions introduced in the LECRIM on the use of IT measures in criminal investigations, by way of the legal reform of 5 October 2015[28]. Thus the criteria for assessing the proportionality of the telecommunications interception and access to stored telecommunications, which have to be assessed by the competent investigating judge in each case are now explicitly set out in the different subparagraphs of the lengthy Article 588 LECRIM.

Since this legal reform entered into force[29], the elements to be taken into account for assessing the proportionality of the measure

---

Huvig v. France, 28 September 1995; ECtHR, Kruslin v. France, 24 April 1990; ECtHR, Malone v. United Kingdom, 2 August 1984; ECtHR, Klass v. Germany, 6 September 1978.

See also J. McBRIDE, *Proportionality and the European Convention on Human Rights*, in E. ELLIS (ed.), *The Principle of Proportionality in the Laws of Europe,* Hart Publishing, Oxford, 1999, p. 29 ff.

[25] See e.g., N. EMILIOU, *The Principle of Proportionality in European Law: A Comparative Study*, Kluwer International, London, 1996, p. 23-24.

[26] The Court applies here the rule set out by Alexy, that the greater the degree of non-satisfaction of, or detriment to, one interest, the greater must be the importance of satisfying the other: R. ALEXY, *A Theory of Constitutional Rights,* Oxford University Press, Oxford, 1986, p. 102.

[27] See STC 14 December 1995, n. 48/1995; STC 29 July 1986, n. 108/198; STC, 7 November 1983, n. 90/1983.

[28] On these provisions see generally L. BACHMAIER WINTER WINTER, *Access to Telecommunication Data in Criminal Justice: Spain,* in U. SIEBER-N. VON ZUR MÜHLEN (eds), *Access to Telecommunication Data in Criminal Justice,* Duncker & Humblot, Berlin, 2016 p. 647-704. See also R. GARCIMARTÍN MONTERO, *Los medios de investigación tecnológicos*, Aranzadi, Cizur Menro, 2018.

[29] The law entered into force on the 6th December 2015.

of telecommunications interception are set out in Article 588 *bis* a) LECRIM, paragraph 5: «The investigative measures covered in this chapter are only deemed proportional when taken into consideration all the circumstances of the case, the limitations of the rights and interests affected do not exceed the benefits of their adoption for the public interest or the interests of third parties. For the weighing of the conflicting interests, the public interest will be assessed taking into account the seriousness of the crime, its social significance or the technological sphere where it has been committed, the intensity of the existing evidence and the importance of the possible information or evidence sought by the measure restricting the right».

Art. 588 *septies* a) LECRIM regarding the search of computers (mass storage devices) states that the judicial authorization shall define the scope of the search and also determine if the digital data can be copied and how these copies are to be preserved.

In traditional searches of homes or other premises, only those elements of evidence that are related to the crime under investigation can be subject to seizure. The problem with the search of computers – direct or remote, at this point there is hardly no difference – lies in the way the data may be stored, where irrelevant data may be kept together with those data that fall within the scope of the search warrant.

The retrieval of digital data usually involves transferring all data through a cloned copy of all the files, or at least the type of files identified in the judicial warrant (for example, only e-mails, or only pictures). Once the data stored in the searched computer have been retrieved and copied, the IT law enforcement officers should focus on the search of the digital data specified in the judicial warrant.

The problem arises because some judges are not able to differentiate the type of digital data that are needed, and the law does not impose the obligation to use targeted search tools. In practice they are used, because of time and financial constraints, but the search engines or how these forensic tools should be applied, or who should control its use, are questions that need to be addressed, as they directly affect the principle of proportionality [30]. Moreover, taking into account that searches of computers affect not only the

[30] As I already pointed out in L. BACHMAIER WINTER, *Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy*, in *Zeitschrift für die gesamte Strafwissenschaft (ZStW)*, vol. 129 (2017), i. 1, p. 1-27, p. 23.

rights to privacy, data protection, and confidentiality of communications of the computer's owner or user but also the right to privacy of numerous persons completely unrelated to the crime, proportionality principle should be very strictly scrutinized. Spanish law insists on compliance with the specificity and proportionality principles in granting and executing the measure, but it does not say anything about how these principles are to be respected in the search of computers.

The rules introduced in 2015 also establish a strict penalty threshold for the type of offences where telecommunications interception is allowed, and thus *sensu contrario*, if these requirements are not met, the measure would not be proportional, and therefore unlawful. However, this threshold, as will be explained below, does not apply when the crime has been committed in the digital environment, and thus the access to the computer data and communications is the only way to investigate it and to fight against impunity, even if the crime committed is not grave.

3.3. *Search and seizure of digital data: the legal framework*

Digital investigations can be carried out on any kind of mass storage devices. Article 588 *sexies* b) LECRIM as of 13/2015, of 5 October, mentions specifically computers, communication instruments or devices of mass data storage, and access to digital data repositories. The requirements are not essentially different, but the differences are determined by the characteristics on the access to digital data, as the search of a mass storage device can include communication data and the quantity of data seized are obviously much broader than would result from a search of premises, where the proportionality principle can be directly applied (mutatis mutandis, plain view doctrine). Otherwise, necessity, proportionality, and judicial warrant requirements are equally required.

The lengthy new articles 588 *sexies* (a), 588 *sexies* (b), and 588 *sexies* (c) LECRIM provide a complete regulation of the search and seizure of digital data, specifying all the requisites for its legitimate use.

Article 588 *sexies* a) LECRIM mentions several of those data specifically. This rule requires specific individualised grounds for such measure. The rules on search of computers and other mass storage devices are as follows:

Article 588 *sexies* b) (access to information of electronic devices

seized outside the home of the suspect/defendant). «The requirement set out in paragraph 1 of the preceding Article shall also apply to cases in which computers, communication instruments or devices of mass data storage, and access to digital data repositories, are seized independently from a house search. In such cases, officials shall inform the judge of the seizure of such devices. If the judge considers that the access to the information hosted in such devices is absolutely necessary, he may grant the corresponding authorization».

Article 588 *sexies* c) (Judicial authorization). «1. The judicial warrant authorizing access to the information contained in the devices this section refers to, shall determine the conditions and scope of the search and may authorize the copying of the computer data found. It shall also determine the conditions necessary to ensure data integrity and preservation guarantees to enable, where appropriate, the examination by an expert for preparing an expert opinion.

2. Unless they constitute the object or instrument for committing the crime or there are other reasons that justify the seizure of hardware containing computer data or files, the confiscation of the hardware will be avoided, when this would cause serious damage to the user or owner and it is possible to secure the data by obtaining a copy of them in conditions that guarantee the authenticity and integrity of the data».

An extended search of other computers connected to those placed in the domicile under search is also regulated under paragraph 3 of this Article, but it needs to be authorised specifically by the judge, if not foreseen initially.

In cases of urgency, this same paragraph allows: «in case of urgency, the Judicial Police or the prosecutor may carry out the extended search of computers, informing the judge immediately, and in any case within the maximum period of twenty-four hours, of the action taken, the manner in which it has been carried out and its results. The competent judge, also in a reasoned decision, shall revoke or confirm such action within a maximum period of seventy-two hours» (Article 588 *sexies* c) paragraph 3 LECRIM).

Under paragraph 4, there is also a temporary derogation for the previous judicial warrant in cases of urgency for the search of mass storage devices. Paragraph 4 of Article 588 *sexies* c) LECRIM reads:

«In cases of urgency, where a legitimate constitutional interest that makes the measure envisaged in the previous sections essential, is present, the Judicial Police may carry out the direct examination of the data contained in the seized device, communicating it

immediately, and in any case within the maximum period of twenty-four hours, to the competent judge in a reasoned writing, stating the reasons that justified the adoption of the measure, the action taken, the manner in which it was carried out and its results. The competent judge, also in a reasoned decision, will revoke or confirm such action within a maximum period of 72 hours after the measure was adopted».

The rules introduced by Organic Law 13/2015 on interception of telecommunications and access to stored data do not provide for different requisites, duration or formal requirements for real-time communications and stored digital data (communications or not). The LECRIM seems to regulate in general access to stored data regardless if those data are communications or not; and moreover, it applies to them considerations of intervention of communications, rather than considering these measures as access to documents. In short, in this precise aspect the rules of the LECRIM are unclear, because when regulating access to stored electronic data in computers or other electronic devices, it does not distinguish between ordinary (non-communications) digital files and stored communications. According to the judgment of the Supreme Court of 23 October 2018, n. 3754/2018 [31]: «The Legislator in a positive way has chosen to grant a unitary treatment to the data contained in computers and mobile phones, that show the personal profile of the person under investigation, protecting so the newly recognised constitutional right, the right to the protection of the virtual environment itself».

As can be seen, the requisites are regulated in a very detailed way, in particular regarding to the content of the judicial warrant authorizing the search and seizure, the limits to the seizure of computer hardware and the way to make copies of the digital data seized. The LECRIM requires a specific warrant to authorise the search and seizure of mass storage devices and the seizure of digital data, underlining that these searches are not covered by the judicial warrant authorizing the enter and search of premises [32].

---

[31] In the same sense, recognizing the newly created constitutional right to the protection of the digital environment, see already Sentencia Tribunal Supremo (hereinafter: STS), 18 July 2014, n. 587/2014; STS, 24 February 20124, n. 587/2014; STS, 17 April 2013, n. 342/2013.

[32] Article 588 *sexies* (a) LECRIM (Need for specific motivation).

«1. When it is foreseeable that during a domicile search the apprehension of computers, telephone or electronic communications instruments, mass storage digital

Spanish LECRIM regulates also the remote access to computers, without differentiating between the access to communications and to other digital files [33]. On the other side it specifies the possibility of remote access, without clarifying if it means cloning remotely the device accessed or including also the possibility to keep a live monitoring of the device [34].

3.4. *The protection of digital sensitive or privileged information*

Professional privileges were protected in the LECRIM originally only under the form of testimonial privilege. Article 416 LECRIM provides testimonial privilege as follows:

«Following persons are exempted from the obligation to testify:

1. The relatives of the accused in direct ascending and descending lines, spouse or relationship analogous to marriage, their brothers or half blood and collateral blood relatives up to the second degree and relatives referred number 3 of Article 261.

The investigating judge has to warn the witnesses of the preceding paragraph that they are not obliged to testify against the accused; but can make the statements they deem appropriate.

2. The lawyer of the accused, regarding the facts that he had trusted him in his capacity as defender.

3. The translators and interpreters with regard to the conversations and communications between the accused and the persons mentioned in the preceding paragraph, in relation to the facts to which he was referred for translation or interpretation».

And Article 417 LECRIM states that the following persons may not be obliged to testify: 1) priests, pastors or religious ministers, with regard to the facts entrusted them in the exercise of their

---

information devices, or the access to electronic data repositories will take place, the judicial warrant authorizing the search of dwellings shall extend its reasoning to express the reasons, if any, that authorize the agents to access the information contained in such devices.

2. The simple seizure of any of the devices mentioned in the preceding paragraph, carried out during the home search, does not authorize to access to its content, notwithstanding the possibility that such access could be authorized later by the judge».

[33] On the regulation of the remote access to computers, see L. BACHMAIER WINTER, *Remote search of computers under the new Spanish Law of 2015: proportionality principle and the protection of privacy*, cit., p. 2 ff.

[34] *Ivi,* p. 24.

pastoral functions; 2) public officials subject to state secrecy [35]; and 3) morally or physically incapacitated persons (the expression «morally» incapacitated is to be understood as mentally disabled).

Despite not being mentioned in the LECRIM, journalists cannot be obliged to give information or testify about their sources of information, as this professional secret is granted constitutional protection under Article 20.1 of the Spanish Constitution.

Organic Law 13/2015, of 4 October introduced specific protections to the communications between the defendant or suspect and her defence lawyer. Such communications were already protected by the case law of the Supreme Court [36] and by the Constitutional Court, on the basis of the constitutional right to defence envisaged in Article 24 Spanish Constitution [37]. Relevant is the decision of the Supreme Court in a corruption case where the conversations between the imprisoned defendant and his lawyer where intercepted (and later declared illegal), where the Court held: «In the event that the legal system did not respond rigorously to such a serious violation of fundamental rights, no defendant remanded in custody and no lawyer would have from now on, when they talk in a prison visiting room about the defence strategy and other issues related to procedural and personal problems of the accused, the minimum guarantee that their conversations were not overheard» [38].

As a rule privileged communications – lawyer and client, journalist etc. – cannot be intercepted, save the exception made by the penitentiary rules in terrorism cases; and when the crime-fraud exception applies, where there is objective evidence indicating that the lawyer took part in the criminal activities under investigation, or of the involvement with the suspect or accused in committing another criminal offence, without prejudice to the provisions of the penitentiary law. Article 118.4 LECRIM (as amended by O.L. 13/2015) reads:

«All communications between the investigated or accused and his lawyer will be confidential.

---

[35] The rules on state secrets and classified information are mainly included in the *Ley de Secretos Oficiales* 9/1968 of 4 April 1968, which was amended deeply by Law 48/1978, of 7 October 1978 and later also in 2002.

[36] See, *inter alia*, STS, 9 February 2012, n. 79/2012.

[37] STC, 26 June 2000, n. 175/2000.

[38] Supreme Court Decision (auto), 19 October 2010, n. 12366/2010.

If these conversations or communications were captured or intercepted during the execution of any of the measures regulated in this law, the judge will order the deletion of the recording or the returning of the intercepted correspondence to the recipient, documenting these circumstances in the proceedings.

The provisions of the first paragraph shall not apply when there are objective indications of the lawyer's participation in the investigated criminal act or of his involvement together with the suspect under investigation in the commission of another criminal offence, without prejudice to the rules provided in the General Penitentiary Law».

The Supreme Court limits these cases to those in which «there is evidence, sufficient and adequately checked, that the lawyer has overreached his duties and responsibilities, joining the criminal activity as one of its members» [39]. Even if this is the case, special precautions must be taken when intercepting lawyer's communications since this measure may compromise the information and data of the lawyer's clients (even from people with no relation to the criminal proceedings in progress). Therefore, courts have stated that the authorizing judge has to be particularly careful with respect to the principle of proportionality, weighing if the investigative purposes really justify the interference of communications protected by the right of secrecy.

Thus, as set out under Article 118.4 LECRIM the general rule is that the lawyer's communications cannot be intercepted, except when he is the suspect himself [40]. Beyond that, there are no provisions on how to prevent that when carrying out a digital search, the data covered by legal privilege are segregated adequately to ensure the constitutional protection of the confidentiality of these communications [41].

The LECRIM does not provide any other special rules on how to protect lawyer-client privilege (or other professional privileges) in

---

[39] STS, 28 November 2001, n. 9296/2001.

[40] The legal reform of Article 118.4 LECRIM follows the same principles set out already in the German criminal procedure, when interpreting section 100 and 148 of the *Strafprozessordnung*. See the judgment of the BGH (*Bundesgerichtshof*) of 5 November 1985, 33, 347.

[41] On the need to provide clear safeguards at the EU level to prevent that these communications are intercepted, see See L. BACHMAIER WINTER, *Introduction,* in L. BACHMAIER-S. THAMANN-V. LYNN (eds.) *The Right to Counsel and the Protection of Attorney-Client Communications in criminal proceedings. A Comparative View*, Springer, Cham, 2020, p. 2.

digital searches. With regard to the measure of entry and search of lawyer's office, even if there is no specific provision the Rules on the Bar state that the dean of the relevant bar association could be required to be present during the search of the lawyer's office to ensure the protection of professional confidentiality. Supreme Court in the judgment 9727/1994, of 27 April stated that the search of lawyers' offices needed to be carried out with extreme care, and considered the presence of the representative of the bar association as an essential requirement, while other decisions have considered that this requirement was not needed for the validity of the search [42].

Guidance on the search of law offices can be found in Report 10/2015, of 14 December of the Spanish Bar Association: a) avoidance of useless inspections, both regarding the content and the duration; b) avoidance of unnecessary damages; c) adoption of additional precautions such as requesting the list of persons whose files or documents could be subject to seizure, in order to ensure compliance with lawyer-client privilege. The Report expresses serious concerns on the possibility foreseen under the new Art. 588 *septies* a) LECRIM of carrying out remote searches of computers.

In practice IT units expressed that the way to proceed to prevent infringement on these rights are as follows: if they know beforehand the name of the defence lawyer, they exclude those mails from the search. But obviously this has only a protective impact, when those data are known. LEA admitted that as for now there is no possible way to avoid that digital data protected by professional privilege are not seized, as the cloning or mirroring covers the whole content of the device seized. Scholars have already stressed this lack of tools for segregating privileged data or involving an independent authority to overlook the proportionality of the searches of computers [43].

3.5. *Procedures for specific phases of digital investigations*

a) Procedures for phase 1 and 2 (acquisitive and investigative stages)

Regarding the acquisitive process or Phase one of the collecting of digital evidence, the procedures regarding on how the DEFR (digital

[42] Decision (auto) of the Constitutional Court, 7 July 2000, n. 167/2000.

[43] See precisely L. BACHMAIER WINTER, *Remote search of computers under the new Spanish Law of 2015*, cit., p. 23-24.

evidence first responder) and the DES (digital evidence specialist) should proceed in the initial stages of the collecting of the digital evidence, have evolved rapidly since standards on how to proceed have been adopted. However, several years ago and before entering into force the precise rules on electronic evidence of 2015, it was not infrequent that the cloning and analysis of the data contained in the seized devices was done in the investigating judge court rooms, at the presence of the judicial notary, who has to be present at the opening of the sealed boxes or bags containing the devices and the cloning. As some judgement of the Supreme Court shows, this was a common practice [44]. So far this might be considered also correct under present standards, as long as the seized device is kept protected in the approved sealed bags (Faraday bags), and the breaking of the seal and cloning is done in the presence of the court notary.

In the past the analysis of the data were also done in the court's premises, something which is not acceptable anymore. Despite the lack of legal rules on this, the applicable standards provide for the detailed proceedings that have to be followed. The UNE standards list all the tasks that have to be documented in Phase one. These standards, which are very similar to the ISO and ENFSI (European Network of Forensic Science Institutes) standards, state:

«All forensic analysis requires a quality control of the acquisition of the data or samples that will be subject to forensic analysis, which implies the traceability of the chain of custody. To this end, all the procedure carried out must be documented from the moment the analysis begins until its completion, indicating the processes and tools used as well as the moment in which each one was executed, following a clearly defined time sequence.

A record must be kept and it must be auditable. Consequently, the traceability and the chain of custody of digital evidence must have a document management system in place where all the steps carried out by the IT staff are reflected. This system must be implemented in electronic or paper format, and it must be collected from the

[44] As shown by the Supreme Court judgment of 3 October 2017, n. 3463/2017, where reference is made to the search of data contained in a computer carried out in the office of the judicial notary in 2012. In that case, the defendant challenged this digital evidence analysis, and the Supreme Court considered that no infringement of the right to defence had been caused to the defendant in that case. The decision might have been completely different at present.

initial process of acquisition of the digital evidence until the completion of the corresponding expert through the drafting of the expert report. The document management, by way of recording auditable events of the chain of custody, entails a series of documents or forms that must be prepared by the staff that performs the forensic analysis itself.

The document management of the chain of custody must include, among others, following documents and record of activities:

– the register of the digital evidence / samples received that are to be analysed.

– a record of the documentation received. The documents that must accompany a digital evidence can be the following:

– description of electronic evidence; the chain of custody until arrival in the forensic analysis lab; forensic analysis requested; necessary authorizations to carry out the requested studies;

– record of the description of the digital evidence, which describes in detail both the digital evidence and the state in which it has been received;

– initial handling record: the forensic data cloning or mirroring process must be detailed;

– record of the status of evidence/samples. This document should reflect the operations carried out on a digital evidence, where these operations are carried out, by whom and the time at which they are carried out;

– documenting the tasks of the initial analysis;

– documenting the tasks of the definitive data analysis indicating the different processes that are carried out, as well as of the temporary location of the evidence if the study of it is temporarily suspended».

The checklist is available to the DEFR and DES, and in principle, it should be known and followed by the officers intervening in phase one.

The practice in documenting the whole process may differ, depending the circumstances under which the devices where found and seized. It depends also if the device is running or it is off; if it is connected to a network or not; if it can be seized or not.

If during the search of premises the judicial notary is already present, and the device should not be seized, the cloning could be done immediately. If the device should be seized, and the judicial notary is not present, it will be put in the sealed bag and transported to be cloned later at the presence of the judicial notary, unless there is urgency in cloning the device at the spot. In

such case, the LEA shall do it. When carrying out the measure of enter and search, whenever possible IT officers shall take part in it, so that the decisions on running devices, on how to keep them connected/protected and on assessing the urgency in cloning the data can be taken immediately. In practice, however, the cloning is frequently done at the spot, and the sifting and analysis of the data is hardly done on site, due to time and other practical constraints. Analysis is done off site almost always in criminal investigations (we have no information on administrative antifraud investigations).

Article 588 *sexies* c) LECRIM defines what shall be the content of the judicial warrant authorizing the search of a massive storage device. In its paragraph 2 it states:

«Unless they constitute the object or instrument for committing the crime or there are other reasons that justify the seizure of hardware containing computer data or files, the confiscation of the hardware will be avoided, when this would cause serious damage to the user or owner and it is possible to secure the data by obtaining a copy of them in conditions that guarantee the authenticity and integrity of the data».

As happens with phase 1, the statutory law does not provide any rules on documenting the precise steps taken in phase 2 (investigative process) regarding the digital evidence, but the standards mentioned already and followed by LEA IT staff do require such reports. The analysis of the data within the investigative stage is to be documented by the IT staff, the DEFR.

b) The digital forensic laboratories

The international standards establish that the investigative process of the digital evidence should ideally be carried out in specifically equipped IT forensic laboratories. The information obtained regarding such equipment was not complete. It was assured that such labs exist and that, when established, they comply with Interpol IT forensic standards. In central IT units of the LEA it is for sure that they exist and most probably comply those standards, although we have not accessed to them. To what extent such labs exist along the Spanish geography is not determined. Information received from the *Comisaría General de Policía Científica*, confirmed that although they follow the ENFSI, no one is certified according to ISO standards or other national

accreditation institution [45], and it could not be established how many of them exist in the whole Spanish territory.

c) The synthesis of an explanation, within agreed limits, for the factual information about evidence (the interpretation of the analysis)

The scope of the digital investigation is defined by the investigating judge authorising the search of the computer or other device. As mentioned earlier, Article 588 *sexies* c) LECRIM, in its paragraph 1 states:

«1. The judicial warrant authorizing access to the information contained in the devices this section refers to, shall determine the conditions and scope of the search and may authorize the copying of the computer data found. It shall also determine the conditions necessary to ensure data integrity and preservation guarantees to enable, where appropriate, the examination by an expert for preparing an expert opinion».

Information provided by the relevant police unit (*Policía Científica*) confirms that they prepare their reports and expert opinions following the already mentioned standards. Within the UNE standards, there is a detailed description on what are the processes and information to be checked at the examination stage and reflected in the report. The standard includes a list of data, actions and processes that should be included in the report, although the list does not pretend to be exhaustive as it may include other data and actions:

«A detailed forensic analysis of electronic evidence, without being exhaustive, should contemplate the following studies:

1 Determination of system information: hardware installed and recognized by the operating system, date, time and user of the last system activity, regional configuration data, etc.

2 Study of the physical devices connected at some point to the computer equipment: digital personal agendas, mobile phones, memory sticks, printers, scanners, multifunction equipment, cameras and video cameras, memory cards and other external storage units.

3 Study of the desktop or main display screen and its recycle bin.

[45] The information received is somewhat confusing because it says «no-one is accredited», so that it is unclear if it refers to the laboratory or to the IT DEFR. I have interpreted that it refers to the laboratory.

4 Network connections and cards installed with MAC identification, in addition to the protocols used and IP addresses.

5 Study of the communications from the computer equipment.

6 Study of the system registry and audit logs of the operating system itself.

7 Information contained in the spaces not allocated in the partitions and in the physical space not occupied by the logical files, which include areas or disk space not currently allocated by the system.

8 Information contained in hibernation, paging, partition and swap files, etc.

9 Printer queue analysis.

10 View links to files, as well as recently accessed files.

11 Study of the folders of the different users.

12 Study of installed applications related to programming, recording and image processing, audio, image and video processing, accounting and economic management software, office automation programs, etc.

13 Study of metadata, when they are of interest.

14 Analysis of virtualization applications, in order to determine the virtual media created and their configuration.

15 Study of installed databases and their management systems.

16 Study of encryption software and encrypted files and partitions, as well as the possibility that it will be implemented in the operating system.

17 Study of Internet browsing, with determination of "cookies" and analysis of the different folders that present browsing history in said network.

18 Analysis of emails and emails via the web.

19 Analysis of instant messaging records and conversations (known as "chats"), along with contact lists».

d) Obligation to record/document the procedures

There is no legal provision requiring the recording of these procedures, but it is established in the adopted standards. Nevertheless not all standards specify the obligation to record all procedure on an electronic archive, but this is how it is done in practice. In case of objection of the integrity and authenticity of the digital evidence, the recording of the procedure will be crucial for the assessment of the digital evidence.

The data should be located in the archives of the *Policía Científica,* but this information was not confirmed, as it was not confirmed what security measures are in place to ensure the data protection rules. In any event, these files are subject to the general provisions on data protection, as foreseen in Organic Law 3/2018 of 5 December of Data Protection and Safeguards of Digital Rights and in the Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [46].

e) Data retention

According to the Resolution of 30 June 1995 issued by the General Directorate of the Police a distinction must be made between three different types of data, depending the actions they are related to (not if they are digital data or not):

a) Police actions carried out within State security or within the fight against serious forms of organised crime (terrorism, drug-trafficking, money laundering, and all other criminal acts committed by organised groups). These data are not subject to the application of the safeguards and requirements established in the Organic Law for Data Protection.

b) Police actions aimed at the prevention of other real dangers, not included in the previous paragraph. The personal data obtained within these investigations shall be cancelled by the police within 5 years of the moment the last data was added.

c) The police actions developed in the field of criminal repression and investigation which have required the use and storage of personal data will be cancelled within five years when the criminal proceedings ended with a conviction sentence. The time limit will start to run the moment the penalty has been enforced.

[46] OJ L 119, 4 May 2016, p. 89. At the moment of finalising the present study the transposition of this Directive into the Spanish legal framework is still pending, although the time limit ended on the 6 May 2018. The Ministry of Justice has recently presented a draft law to implement this Directive.

As to the digital data within the judicial proceedings, Article 588 *bis* k) LECRIM provides for the destruction of data in the following way:

«1. Once the criminal proceedings are terminated by a final ruling, the original records that are kept in the electronic and computer systems that have been used in the execution of the measure, shall be deleted and erased, upon order. A copy of those records will be kept under the custody of the judicial notary.

2. The preserved copies will be destroyed after five years have elapsed since the sentence was executed or when the time for the statute of limitations of the offence or the prosecution has expired or the decision to put an end or sentence of acquittal is final, unless the court considers its conservation necessary.

3. The Court shall instruct the Judicial Police to put into effect the destruction referred to in the preceding paragraphs».

Some scholars have criticised this provision because it still allows the court to order the conservation of the intercepted conversations («provided that the court does consider the conservation necessary»)[47]. On the other hand, this provision does not establish who shall decide on the destruction and check that it has being done, because it is not clearly stated who is the authority responsible for storing the evidence and then controlling its destruction.

3.6. *Cooperation with OLAF in digital investigations*

The investigations on PIF crimes, where cooperation with OLAF is not only frequent, but is the rule, are carried out mainly within the Special Anti-Corruption Prosecution Office (*Fiscalía Anticorrupción*) with the support of the specialised unit of the judicial police on economic and fiscal crime (UDEF, *Unidad de Delincuencia Económica y Fiscal*). Taking into account the fluid and close relations between OLAF and the Spanish *Fiscalía Anticorrupción*, it would be expected that they may also exchange best practices on digital forensic procedures in antifraud investigations. Nevertheless, this would not change much the Spanish practice, because as it was

[47] I. OUBIÑA BARBOLLA, *Datos personales y nuevas tecnologías de investigación tecnológica: oportunidades, retos y límites*, in I. COLOMER HERNÁNDEZ (dir.), *Cesión de Datos Personales y Evidencias entre Procesos Penales y Procedimientos Administrativos Sancionadores o Tributarios*, Aranzadi, Cizur Menor, 2017, p. 221-277, p. 276-277.

explained, those standards are essentially complied with, being similar to those set out in UNE, ISO and ENFSI 2015.

4. *Investigating authorities (DEFR, DES)*

This part focuses on the persons that shall or can carry out digital investigations and their expertise, both in criminal and administrative punitive proceedings. In the Spanish system there are no specific legal provisions in the Code of Criminal Procedure for digital investigations, and the legal framework does not determine which officer shall intervene in phase one and phase two of the digital investigation. Thus the general rules on criminal investigation apply. However, in practice the relevant investigating units have adjusted their actions to the applicable standards. Nevertheless, this practice may not be completely uniform along the Spanish territory.

Information obtained from the practice shows that the seizure of devices is usually done by the operative units of the LEA and the cloning of the content of the seized devices is to be done with presence of the judicial notary, but it is unclear if at this stage the DEFR is staff from the relevant judicial police unit or from the *Policía Científica.* The persons working on phase one are usually not the same persons that are in charge of phase two, although in some cases, specifically in complex economic crime investigations or when the computers cannot be disconnected from the network (e.g. banks), then the IT analysts will intervene already in phase 1.

Analysis and reports are done by the relevant unit of the *Policía Científica,* unit on IT forensics. The first expert reports in this field started to be elaborated in 1999. Over time a Group of IT forensics was set up and in 2008 it became a formal unit. The IT Forensics Section was organized into three groups: 1. Software analysis unit; 2. Electronics unit; and 3. Mobile forensics unit.

Royal Decree 952/2018, of July 27, which develops the organic structure of the Ministry of Interior, provides that the IT forensics unit works within the *Comisaría General de Policía Científica*. The latter is part of the *Dirección Adjunta Operativa*, which depends on the General Directorate of the Police. Above this unit there is the *Secretaría de Estado de Interior*, which is under the direct orders of the Ministry of the Interior.

Order INT/28/2013, of January 18, which develops the organizational structure and functions of the Central and Peripheral

Services of the General Directorate of the Police, in its article 10.3 provides:

«Article 10. *Comisaría General de Policía Científica*.

It will consist of following units:

3. Central Unit of Criminalistics. (Unidad Central de Criminalística)

It will have the functions of preparing expert reports, which are of police and judicial interest, with regard to falsification of documents, graphoscopy, identification, operational forensic ballistics, analysis of traces, forensic acoustics and IT forensics, as well as the elaboration of expert reports related to the matters within its competence».

As to the DES, the Spanish legal system requires the involvement of an expert in digital forensics, in application of the general rules in witness expert evidence and reports. Therefore, as already mentioned, the expert evidence within the criminal investigation shall be provided by the IT experts of the *Policía Científica* in those cases where they are involved (as they do not act in all cases involving IT evidence and investigations). In addition to the official expertise prepared by the public scientific institution within the police structure, Spanish criminal procedure allows that expert evidence is presented at the initiative of the defendant or any other private accusing party, at their own costs. In conformity wit the general rules on appointment of expert witness by the parties to the proceedings (Art. 471 LECRIM), the expert witness shall have the necessary degree that credits his/her education and expert knowledge.

Thus, when it comes to digital evidence, such expert reports have to be prepared by an IT expert with the relevant degree and registered in the official association. Nevertheless, the rule admits that persons without an official degree exceptionally undertake the reports and analysis, e.g. there is no certified expert available or the expert shows enough qualifications even if he/she is not in possession of an official degree in computing. Rules on expert evidence in the LECRIM (arts. 456-485) date back to 1882, and thus they have been interpreted to adapt to the present requirements and standards.

As a rule to be admitted to the professional associations for IT forensic experts (these associations are public institutions guaranteeing the professional quality/degrees and standards, both technical as deontological), a university degree on computer engineer or technical IT engineer is required. This is necessary as a

rule to be appointed as private IT expert. Within the scientific police unit, as a rule the IT staff will also hold a degree in computer science, or specific training courses in the police academy. The professional qualification of the IT expert should be accessible to the defendant, but in general a person working for the scientific police usually will not be challenged for its lack of professional skills or lack of certificate, due to the competitive recruiting process which ensures a high level of quality. Despite the continuous training on the latest IT developments, it cannot be excluded that some officers are not sufficiently skilled. Their qualifications and certifications can be challenged as with regard to any other expert evidence. Any expert can be subject to recusal if there are elements that cast doubt on his/her impartiality, and during the trial the results (and also the methodology and thus the qualifications of the expert) are subject to cross-examination, as any other evidence (Arts. 723-725 LECRIM). Challenging the skills of the IT police units is rarely done in practice. Lawyers do not follow such strategy which is doomed to fail, as the IT experts of such units have general professional recogniton.

5. *Defence and third party rights*

This part focuses on the subject of the proceedings (e.g.: the target of the administrative investigation/defendant), as well as of third parties potentially involved in the investigation, and of their rights, both in criminal and administrative punitive proceedings.

5.1. *Main defence rights and procedural safeguards*

Spanish LECRIM grants extensive defence rights to the suspect from a very early stage of the investigation, with full access to the file, save for the acts declared secret. From the moment a person is under investigation (*investigado*), the full range of defence rights arise, not being necessary to be formally charged (Article 118 LECRIM). The rights of the person under a criminal investigation include inter alia, the right to be informed of all the investigative acts carried out against him, the right to be present in the practice of investigative acts accompanied by his lawyer (article 333 LECRIM); to request the practice of investigative acts and also ask for securing evidence; and to object or question the results of such

investigative acts and file remedies against them, to prevent his indictment [48].

The suspect/accused shall be informed of his rights following the detailed list of the content of such information under Article 118 LECRIM (which was amended to adapt to the EU Directive 2012/13/EU on the right to information in criminal proceedings) [49].

The information shall be done in a comprehensive way, making it understandable to the suspect and adapting the language to the age and capacities of the defendant. These rights apply in digital investigations in the same way as with regard to any other investigative acts. There is no special provision for digital investigations. This means that the defendant is to be informed of any investigative act as soon as this does not harm the aims of the proceedings, and the latest when there is an indictment.

Regarding the digital investigation of computers seized, first the defendant has the right to be present during the measures of enter and search of her domicile (Article 569 LECRIM), and as a rule in practice she will be present as well as the defence lawyer. If the computer is located there, she will have knowledge of its seizure at that very moment.

Second, the defendant has the right to be present when the data is extracted in the presence of the judicial notary. The Guidelines of the General Public Prosecutor on the search of IT devices [50] indicate that taken into account that the judicial notary is already present during the home search, her presence should also ensure the integrity of the digital data, by checking how the search and filtering of the digital data is done. However, the presence of the *Letrado de la Administración de Justicia* is not required by the jurisprudence for the cloning of the computer as the hash should already ensure the

[48] The interest of the suspect under investigation in challenging the validity of the investigative acts at this stage of the proceedings was already recognised by the Constitutional Court in its judgment of 17 April 1989, n. 66/1989.

[49] Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings, OJ L 142, 1 June 2012, p. 1-10.

[50] Circular de la *Fiscalía General del Estado* of 6 March 2019, n. 5/2019, *sobre el registro de dispositivos informáticos*, states that the presence of the *Letrado de la Administración de Justicia* during the entry and search of the home should be used to guarantee also the authenticity and integrity of the digital data.

integrity of the data [51]. As to the analysis of those data, the general rules as explained above, shall apply.

In the context of the digital investigations, it can be questioned whether the defendant and his lawyer have a right to be present during the analysis of the computer data, and whether access to the forensics lab is foreseen. Currently the right to be present applies only at the moment when the cloning or mirroring of the computer is done during the search of dwellings, but not in the forensic lab.

Being present during the home search, the suspect/defendant or the third person who holds the data can consent to its access. In such case the judicial warrant assessing the necessity and proportionality of the measure is not needed. With respect to digital data stored in the cloud, the consent to access them will avoid complex issues on jurisdiction and MLA proceedings, which seems to be problematic in practice, causing delays and additional costs in criminal investigation. There have been problems reported with the identification of anonymous tweets, where the Spanish Public Prosecution claims that they need a legislative reform to oblige ISP companies to provide the required information for prosecuting cybercrime and hate crimes in the internet without having to go through the lengthy and cumbersome MLA procedure [52].

All the investigative acts will be documented in writing and, if necessary, by image/sound recording. The suspect is to be granted access to such reports and receive a copy of them, since he has access to all the materials in the file, unless those are declared secret, because its disclosure would harm the aims of the criminal proceedings (Article 302 LECRIM). The rule is therefore to grant full access to the file unless the measures carried out need to be kept secret for the aims of the investigation. The secrecy of the file needs to be justified, and as a rule it shall only be granted for a month. Certain measures can be kept secret for a longer time, but the secrecy of such measures is to be lifted as soon as it will not hamper the investigation, and when the person under investigation is indicted and at the latest ten days before the pre-trial invstigation is

[51] STS, 14 May 2008, n. 256/2008; STS, 22 May 2009, n. 480/2009; STS, 17 July 2013, n. 342/2013; STS, 23 February 2017, n. 116/2017. Nevertheless, on the possibility to alter in certain cases the hash, see M. MIRANDA YERKO, *Algoritmos HASH y vulnerabilidad a ataques*, in *Informática Forense*, 2010, p. 109.

[52] Made public in the newspapers on 4th July 2020, see *abc.es/espana/abci-twitter-atasca-investigaciones-espanolas-perfiles-anonimos-202007040222_noticia.html.*

closed and the decision to proceed to trial is taken (Article 302 LECRIM).

The defendant has the right to access to the report prepared by the scientific IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions of the expert witness opinion. The official institutes are considered to enjoy neutrality and due to the methodology applied, also reliable. This is the result of applying the general rules on cross-examination and on challenging the expert evidence during trial to digital forensics [53]. The accused can also challenge the results of the official IT expert opinion by presenting a private IT expert opinion. There are no conditions, except the costs for it: private expert opinions will be financed by the accused.

All the safeguards adopted to ensure the authenticity of the digital data, seem to be working in practice quite reasonable, as no special problems have been reported to us. The presence of the judicial notary, the use of sealed bags in the seizure of physical devices, the existence of specialised IT and cybercrime units within the two LEA institutions, the possibility for the defence to challenge the chain of custody, the results, and the production of another scientific expertise by certified IT specialist holding a computer engineering degree, seems to provide for an adequate level of safeguards. The need to provide for a system to safeguard the proportionality principle, the lack of legal rules on the protocols for acquisition/ investigation, and access to the search engines, as well as the broad rules on casual findings, are, in my opinion, subject to improvement and could be revised for ensuring a higher level of protection of human rights in general.

5.2. *Digital evidence ex parte*

Digital investigations carried out by the defendant have evidentiary value, but obviously, the reliability will depend on the prestige and credited impartiality of the relevant expert. There is a difficult question related to the possibility of accessing to the internal compliance investigations of companies by the authorities carrying out the criminal investigation, as there is currently no legal provision in this regard. It is questionable to what extent a legal

[53] Arts. 723-725 LECRIM.

person can be obliged to share the results of its internal investigations; or if the employees who have participated in the investigation can be summoned as witnesses in relation to those investigations. Not revealing the information may save the legal person from immediate reputational damage but entails equally reputational damage if later the acts that entail corporate criminal liability are detected and the company is indicted. In addition it may be also questioned what is the liability of the compliance officer in case of destroying documents discovered during the internal investigation or the report elaborated after carrying out the internal investigations. In the first case. Following Liñán Lafuente, such conduct does not entail criminal liability in Spain, as the destruction of evidence by the perpetrator is not sanctioned independently from the principal crime committed (*autoincubrimiento impune*) [54].

5.3. *Protection of third parties*

When during the search and potentially seizure of digital data rights of third parties are affected, the LECRIM provides for certain rules for the protection of their rights. Until the legal reforms introduced by the O.L. 13/2015, there was no proper protection of the third parties unrelated to the criminal acts whose communications had been intercepted [55]. In particular, third parties are to be notified of such encroachment of their rights. In conformity with Article 588 *ter* i), paragraph 3 LECRIM:

«The investigating judge shall notify the persons involved in intercepted communications the fact of the interference and shall inform them of the specific communications in which they have participated. This information shall take place, unless it should require a disproportionate effort or it could prejudice future investigations. If the notified person so requests, she will be given a copy of the recording or the transcription of such communications, insofar as this does not affect the right to privacy of others or is contrary to the objectives of the proceedings under which the measure was adopted».

---

[54] See, A. Liñán lafuente, *La responsabilidad penal del Compliance officer*, Cizur Menor, 2019, p. 143-147.

[55] See L. Bachmaier Winter, *Intervenciones telefónicas y derechos de terceros en el proceso penal. La necesidad de una regulación legal del secreto profesional y de otras relaciones de confianza*, in *Revista Derecho Procesal*, 2004, i. 1-3, p. 41-82.

This provision is to be welcomed. However, as the exceptions for complying with this duty are so broadly drafted, in practice it may lead to a generalised lack of information. It has to be noted that the notification of the conversations held by a third person in most cases will «affect the right to privacy of others», unless the conversation was with one of the defendants.

If a third person considers that his rights have been violated, he would be able to claim for a compensation of damages. In the case the interception of the communications were unlawful, it would constitute a crime, under Article 197.1 of the Spanish Criminal Code (*Delito de interceptación de comunicaciones personales*), and the victim would be entitled to a compensation of damages (*actio civilis ex delicto*) within the criminal procedure. If the action is not a criminal action, it could lead to a claim against the State for damages caused in the Administration of Justice.

Article 121 of the Spanish Constitution provides: «Damages caused by judicial errors as well as those arising from irregularities in the administration of justice, shall be subject to compensation by the State, in accordance with the law» [56].

The person whose rights were violated could also press charges against the officer infringing his rights, for such violation could also entail criminal liability under the Criminal Code, as mentioned above.

5.4. *Liability in cases of an unlawful interference in the fundamental rights*

The public official who unlawfully interferes with the fundamental rights of a person, commits a crime. The criminal liability for unlawful infringement on the right to the digital environment (data protection as well as protection of the communications) within the criminal proceedings is provided under Article 539 of the Spanish Criminal Code. The rules on unlawful interception of other communications and the unlawful entering of the home are also of interest here, as they may play some role when electronic data are collected.

The three provisions are enumerated under the heading «Of the offences committed by public officials against the inviolability of the home and other privacy safeguards».

---

[56] This constitutional provision is implemented in Articles 292 to 297 of the Judiciary Act (LOPJ).

Article 534 CC. «1. The authority or public officer who, within criminal proceedings, and without respecting the constitutional or legal guarantees:

1° enters into a home without the consent of the occupant;

2° records any papers or documents of a person or objects that are in her home, unless the owner has freely consented;

shall be punished with a fine of six to twelve months and disqualification from public office for two to six years.

If immediately after registration, the papers, documents and recorded effects are not returned to the owner, the penalty will be special disqualification from public office for six to twelve years and a fine of twelve to twenty-four months, independently from the penalty corresponding to the offence of misappropriation.

2. The authority or public official who, during lawful registration of papers, documents or effects of a person commits any unjust harassment or unnecessary damage to the property, shall be punished with the penalties for these facts, imposed in the upper half and also with the penalty of special disqualification from public office for a period of two to six years».

Article 535 CC. «The authority or public officer, who, within criminal proceedings, intercepts any kind of private postal or telegraphic correspondence with violation of constitutional or legal guarantees, shall incur into the penalty of disqualification from public employment or office for two to six years.

If the information obtained is divulged or distributed, the disqualification penalty shall be imposed in the upper half, as well as the fine from six to eighteen months».

Article 536 CC. «The authority, public official or agent who, within criminal proceedings, intercepts telecommunications or uses any technical devices for eavesdropping, transmission, recording or reproduction of sound, image or any other communication signal, with violation of the constitutional or legal guarantees, shall be liable to a penalty of special disqualification from public office of two to six years.

If she reveals the information obtained, the disqualification penalty will be imposed in its upper half as well as the fine from six to eighteen months».

Within the criminal proceedings, the violation of any fundamental right will lead to the exclusion of the evidence so obtained. Art. 11.1 of the Spanish Judiciary Act (*Ley Orgánica del Poder Judicial,* LOPJ), provides for a very strict exclusionary rule of evidence. It reads as follows: «Evidence obtained, directly or indirectly, in violation of

fundamental rights or liberties, shall have no effect». Regarding the words «the evidence obtained», it was at first thought that Art. 11.1 LOPJ was only applicable when the violation of a fundamental right took place during the preliminary investigation when the evidence was gathered. This was the stance of the Constitutional Court in a decision in 1986, in which it construed Art.11.1 LOPJ in a restrictive way, so that infringements that occurred either at the moment of procedural introduction or testing the evidence would not fall under its provisions, but under those which regulate procedural nullities. This initial interpretation did not prevail in the end. At present the exclusionary rule of Art.11.1 LOPJ is applied to all evidence obtained in violation of fundamental rights, regardless of the moment the violation occurred, be it at the pre-trial stage or at the trial [57].

The defendant can allege such violations already during the pre-trial stage, during the trial, and after the judgment, by way of appeal [58].

If damages have been caused, the defendant will be able to claim compensation for damages for miscarriage of justice (Articles 292 to 297 LOPJ), as explained above. The Public Administration is subject to strict liability in such cases, and the claim for damages has to be filed with the Ministry of Justice. In case of judicial mistake, prior to filing the claim for damages the mistake has to be recognised in a judicial decision. The proceedings for declaring a judicial mistake take the form of the extraordinary review before the Supreme Court. Only then, the Administration would be liable for the damage caused by the judicial mistake. The complexity of this procedure causes that most of the claimants chose to claim damages for miscarriage of justice and not for judicial errors.

6. *Admissibilty of digital evidence at trial.*

6.1. *Admissibility and Reliability of the digital evidence*

Spanish criminal procedure, as it happens in most of the civil law

---

[57] See. L. BACHMAIER WINTER, *Spain: The Constitutional Court's Move from Categorical Exclusion to Limited Balancing*, in S. THAMAN (ed.), *Exclusionary Rules in Comparative Law*, Springer, Heidelberg-New York, 2012, p. 209-234, p. 213.

[58] Any infringement that stems from a violation of fundamental rights and leads to the exclusion of the evidence or the nullity of the investigative act can be alleged at any stage of the proceedings (Art. 238 LOPJ).

systems [59], does not declare unreliable evidence inadmissible: the evidence is admitted and it is for the professional judge to assess its reliability. Certainly in the Spanish system where the information reaches the fact-finder in the form of a one-sided account based on a comprehensive collection of the evidence by an impartial official, leaves only little room for party driven evidence collection. This quasi-unilateral process of evidence gathering, as long as the public prosecutor who conducts it is truly neutral and autonomous – and up to now the Spanish Public Prosecution Service was highly respected for keeping its impartiality – in practice leads to few challenges to the digital evidence. Although the trial is formally structured in an adversarial fashion since the enactment of the LECRIM in 1882, the trial is still to a large extent a stage for testing the veracity of the evidence that was collected in an objective and methodical fashion at the investigative stage. Accordingly, the challenges to such evidence tend to focus more on the legality of the collection and less on the content of the evidence as such.

Digital evidence most often is supported by the relevant IT expert report, and therefore the rules on witness expert evidence apply here. According to the LECRIM (Articles 456 ff.), experts can be individuals or legal persons, public or private. Experts' reports are most often prepared by a highly specialized team of the official forensic institute, as mentioned earlier, regarding digital evidence this will be the Unit on Cybercrime or Digital Forensics, within the *Policía Científica.*

In the Spanish system, the general rule is that forensic reports are made upon request of the investigating judge, when it considers that such scientific or technical assessment is required for the investigation and for finding out the truth (Article 456 LECRIM). In the field of digital evidence it is requested as a rule. Furthermore, the witness experts shall appear in court to present the report and their conclusions at trial, if they are summoned to do it. Forensic expert reports that cannot be carried out by the criminal forensic official institute will be done by private experts, appointed out of a list provided by the relevant professional associations. This is also the way for the defendant to provide for a private forensic digital

[59] See L. BACHMAIER WINTER, *Rights and methods to challenge evidence and witnesses in civil law jurisdictions,* in D.K. BROWN-J.I. TURNER–B. WEISSER (eds.), *The Oxford Handbook on Criminal Process*, Oxford University Press, Oxford, 2019, p. 841-864, at 850.

expertise supporting his/her defence, as has been mentioned above. These experts will be given the means required to carry out the expertise, and they are entitled not only to the reimbursement of the expenses, but also to be paid their fees (official fees). Although in the criminal proceedings it is not frequent that the parties present a private digital forensics expertise, there are cases where the parties request such private expert opinion. And even the official institutions may also request the cooperation of private companies to retrieve data from an electronic device or to determine how the date where destroyed. This was recently the case in a high profile criminal investigation where the current vice-president of the Spanish government has been accused of destroying a sim card of a mobile phone, that was evidence in a criminal investigation. The simcard was sent to a specific lab in the UK to try to retrieve the data stored in it, and alternatively to determine how the card had been destroyed.

Those who are exempt from the legal obligation to testify as witnesses are not suitable to be appointed as expert witness. The official reports prepared by the official forensic laboratories may be presented at the oral trial as documentary evidence (Article 788.2 LECRIM). In order to evaluate the expert opinion as evidence, it is not absolutely necessary that the experts who prepared the report appear in court to ratify their conclusions. The attendance of the witness experts at the court hearing is not required if the parties have not challenged the findings and conclusions of the expertise.

The Spanish criminal procedure model very much influences the main features of the forensic expert evidence: as a rule experts are not appointed by the parties (although the accusing parties different from the public prosecutor and the defendant can appoint their own expert); the state has highly qualified laboratories to provide the necessary forensic expertise in criminal proceedings; as a rule, the expert evidence is paid by the state, for it is prepared upon the request of the investigating judge and its aim is to find out the truth. In practice, the adjudicating body relies on the professionalism and neutrality of the official IT experts, but IT reports prepared by the forensic department of auditing companies are also considered as reliable, as long as they follow the standards for forensic digital evidence.

In sum, the Spanish legal system does not provide for specific admissibility rules. For the digital evidence to be assessed as evidence in criminal proceedings, the general principles on evidence production are to be respected: the evidence has to be produced at

the public trial, and the parties must be granted the opportunity to challenge the legality, authenticity, reliability and integrity of the digital evidence, as well as all other evidentiary materials.

The production of evidence will vary depending on whether it is recorded conversations, recorded images or other electronic data. For digital data, the reading of the transcripts or the reproduction on a computer before the trial court is the usual way to introduce the digital data, or by way of written transcripts. Expert evidence is usually in place too, with the presence of an expert witness to explain the procedure for collecting data and how the integrity, authenticity etc. has been secured through the chain of custody. In the relevant Supreme Court judgment 300/2015, of 19 May of the Criminal Chamber, it was expressly stated that in the absence of expert evidence on the authenticity of the digital evidence, lacking any eye witness who could testify on the truthfulness of the screen captures of the incriminating whatsapps, the evidence was insufficient to override the presumption of innocence of the accused [60].

The general rules and principles on exclusionary rules of evidence shall apply also to the evidence collected through an unlawful access to the digital data. Spanish statutory rules provide for a very strict exclusionary rule. The key statutory provision regarding the exclusion of evidence is Article 11.1 of the Judiciary Act (*Ley Orgánica del Poder Judicial*, LOPJ). The LOPJ enacted in 1985, one year after the Constitutional Court's landmark decision in STC 114/184. This decision clearly influenced the wording of Article 11.1 LOPJ, which reads:

«Evidence obtained, directly or indirectly, in violation of fundamental rights or liberties, shall have no effect».

6.2. *Challenging the authenticity of the evidence and the chain of custody*

Reliability of the digital evidence can be challenged on the grounds that the chain of evidence is not sound, but this will not lead to the exclusion of the evidence. The observance of the processes and safeguards described and analysed in the previous

[60] On this important Supreme Court judgment see F. de la Mata, *La validez de los pantallazos como prueba electrónica: comentarios y reflexiones sobre la STS 300/2015 de 19 de mayo*, *La Ley*, n° 8728, of 23 March 2016, p. 2 ff.

paragraphs as set out in the applicable standards on digital forensics and the process for ensuring the chain of custody, provide for a high standard of safeguards regarding the authenticity of the digital evidence. Although the law does not set out the requirements of the chain of custody, Article 338 LECRIM refers to those standards in abstract when stating that: any object related to the crime shall be collected «in such a way that its integrity is guaranteed» and the decisions on its preservation will be under the control of the investigating judge, the public prosecution and the judicial notary.

Definitions of what constitutes the chain of custody in digital evidence are to be found already in several judgments, as the judgment of the court of first instance SJP Gijón 39/2016 of 6 July 2016 (the acts of collection, storage and transfer of the evidence obtained in the course of the criminal investigation aimed at preserving and guaranteeing its authenticity and indemnity to be used as proof of charge in criminal proceedings, relating it also to the expert evidence when the evidence is subject to further technical study).

The judgment of the Supreme Court 491/2016 of 8 June holds that the purpose of the chain of custody is to ensure that what has been collected and what the court will assess, and the judgment will decide upon, is the same. The processes to ensure that the evidence collected has not been manipulated, altered or tampered.

The role that the chain of custody plays in digital evidence is of outmost importance, due to the volatility of digital data and the possibility to delete them or alter them, easily, if the adequate safeguards are not in place. Breaking the chain of custody can thus determine the invalidity of the evidence since it can lead to the impossibility to ensure its authenticity.

In this regard, the Constitutional Court in judgment 170/2003 of 29 September, in a case where digital data seized from a computer during a home search were not correctly identified and sealed it considered that such "poor control" of the digital evidence could not exclude the existence of possible manipulations or alterations. The court concluded that such violations of the chain of custody processes amounted to a breach of the fair trial rights of the accused. The Supreme Court also has declared that breaking the chain of custody affects the reliability and authenticity of the evidence (STS 491/2016 of June 8)».

But the defendant who seeks to annul the digital evidence produced needs more than simply alleging and infringement of the chain of custody and the potential risks of tampering digital evidence. To challenge the expert reports and the digital evidence,

the defendant may propose an alternative expert evidence and challenge the opinion prepared by the official experts, not being enough to cast doubts on the authenticity of the digital evidence the affirmation of general potential risks of manipulations of the digital evidence to annul the evidentiary value of the produced digital evidence.

Although the regularity of the chain of custody is a pre-requisite for the assessment of digital evidence, «the breach of the chain of custody does not automatically cause the nullity of the evidence, but it serves to cast doubt upon its authenticity» and, depending on the relevance of the infringement, the digital evidence will lose its evidentiary value [61].

The expert report will reflect the compliance of the standards that ensure the chain of custody as well as the reliability of the digital evidence collection, traceability, integrity, etc. by showing compliance with all the protocols and standards applicable. These are elements that need to be explained in the expert report, and this is why it is so important to document each of the steps adopted and each of the actions carried out, as well as the conditions under which the digital data were seized, extracted, transferred, analysed, and preserved. If such information is reflected in the expert IT report (complying the ISO, UNE or ENFSI standards), it will be upon the defendant to proof that such evidence is not reliable and that the chain of custody and other processes have not been respected. And this will require a challenge expert opinion to be presented on his behalf.

6.3. *Accidental findings*

If during a criminal investigation there appear facts relating to another crime, newly discovered facts refer to a crime, which would not allow the adoption of the search of computer, such offence may only be prosecuted on the basis of the accidental findings if it is connected to the principal offence [62].

Article 588 *bis* i) LECRIM as of 4 October 2015, provides for a special rule on accidental findings of another crime during the

[61] STS, 11 December 2012, n. 1072/2012.

[62] Generally on the case law of the Spanish Supreme Court on casual findings, see J. García San Martín, *El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal*, in *La Ley*, n. 4917/2014, p. 1 ff.

execution of a measure of telecommunications interception, which is applicable to the search of computer data [63]. To proceed with the investigation of the newly discovered crime, an additional judicial warrant would need to be requested. And it would only be granted, if the newly discovered offence justifies the adoption of the measure of the search of the computer.

It is only by way of this subsequent judicial warrant that the digital evidence discovered can be used for prosecuting a different crime and the information obtained be used as evidence. Rules on casual findings of evidence during the performance of a criminal investigative action which is restrictive of a fundamental right, allow for opening a further criminal case, on the basis of the information gathered on another possible crime. There is no provision allowing the transfer of such information/evidence to an administrative procedure. Within administrative investigations the rules applicable are those of the Civil Procedure Code, and thus the casual findings that may point to a possible administrative offence, will not be transferred to the administrative authority.

The question whether the digital data collected under a criminal investigation, which lead to the closing of the criminal investigation, could be used as evidence within an administrative sanctioning procedure, is not clear. The general answer would be no, as within the administrative procedure those intrusive investigative measures would not be allowed.

7. *Concluding remarks*

The comprehensive legal reform carried out by way of Organic Law 13/2015 has provided the Spanish criminal procedure with a clear and detailed legal framework on digital investigations and electronic evidence. When it comes to digital forensics, despite the lack of rules in the law, the standards provide for the necessary safeguards and processes to ensure the authenticity and integrity of the digital evidence, as they establish clear rules to be followed at every phase of the criminal investigation. As long as the standards are adopted and followed by Spanish IT experts – both the official IT experts from the LEA and the privately appointed IT experts –, in

[63] On the admissibility of accidental findings as evidence, see, for example, STC 25 March 1996, 49/1996; or STC, 24 February 1998, n. 41/1998.

the different phases (acquisition, investigative, and reporting stages), there should not arise major difficulties in the transnational context either, as the technology for extracting digital data seems to be quite standardised at the international level.

A better regulation as well as a wider harmonization of the legal framework at the EU level on the filtering of data and the selection of keywords, as well as the breath of the searches is, to my mind, still pending. Proportionality principle is clearly at risk, when its protection relies on the lack of time or resources to extend computer searches beyond those data that are strictly necessary. In my opinion relying on practical constraints to protect the citizens against disproportionate interferences in their fundamental rights, is clearly not sufficient. Adequate controls and safeguards should be provided at the legislative level.

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.

Michele Caianiello

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

1. *Digital evidence and financial crimes: General considerations*

Financial crimes represent a privileged field to study the impact of the digital revolution in the management of criminal proceedings, especially with regard to fact-finding and evidentiary issues. For a long time, in fact, this kind of crimes has been usually committed by falsifying documents, or manipulating other real evidence, with the aim to hide unlawful purposes pursued by the perpetrators to the competent authorities, the shareholders, the creditors, the investors, the media and the public opinion.

Also in the field of frauds against the EU budget, the paper trail traditionally left by offenders constituted an essential piece of evidence to which investigators must resort, in order to reconstruct the dynamics of the facts and to bring to justice the responsible

person(s). It is not wrong to affirm that, by tradition, fact-finding in trials concerning crimes against the EU financial interests is prevailingly based on documents: in other words, on written evidence. Oral evidence, on the contrary, plays a complementary role, and it is usually introduced either to explain – under the figure of expert witnesses – what emerges from the papers presented at trial; or to fill the gaps left by the documents, that in their nature constitute circumstantial evidence.

Nowadays, inevitably, in an age of digital economy (and after the advent of the fourth industrial revolution and web 3.0), the "trail" the law enforcement authorities need to follow is constituted by a multiplicity of data, rather than by paper [1]. Finding such trail seems harder than in the past, because data are virtual information whose nature is extremely volatile [2]. Data may be altered, manipulated, modified for a variety of causes (either purposely or because of negligence or lack of adequate training). Furthermore, digital data are usually stored in private devices or other virtual premises not accessible to the public.

This implies that their collection poses significant problems with regard to fundamental rights, especially the right to private and family life [3] and the right to property. Most of all, respect for human dignity may be concerned if we consider how data may reveal information relating to the core area of the individual sphere. In addition, the right to defense must be ensured, because the defendant needs to have an effective chance to challenge the way in which e-

---

[1] See G. LASAGNI, *Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences*, Springer, Berlin, 2019, p. 1; S. BRAYNE, *Big Data Surveillance: The Case of Policing*, in *American Sociological Review*, 2017, p. 980. It may be useful to note that issues concerning the collection and admission of e-evidence are now emerging in many areas of criminal law, due to the digitisation of the economy and all areas of social life. For example, the use of electronic evidence is increasing in the field of international criminal law, where photos, videos, information contained or transmitted through social media are becoming sometimes the main evidence to prove that a crime of international nature has been (or is being) committed. See L. FREEMAN, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, in *Fordham International Law Journal*, Vol. 41, Issue 2, p. 283. As is well known, some philosophers coined a new definition – onlife – to define the pervasiveness of digitisation in every area of our lives. See L. FLORIDI (ed), *The Onlife Manifesto. Being Human in a Hyperconnected Era*, Springer, Cham, 2015.

[2] See *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics: Best Practices and Perspectives*, § 1.

[3] See *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics*, cit., § 7.

evidence was collected [4]. This may require, as a consequence, some additional burden in documenting the investigative operations conducted by law enforcement officers [5].

Hence, summing up the main critical issues illustrated in the previous chapters, prosecuting and law enforcement authorities are required to face a set of problematic steps: first, they need to collect and store the data in an appropriate way, so that their reliability is not undermined. Then, they need to document the investigative operations in a way that does not compromise the right to defense, giving to the defendant an effective opportunity to question the probative value of the information collected. Sometimes this is *per se* difficult, because the massive use of digital devices entails the need to carry out new types of investigative operations, for which it is not easy to identify in advance what are the correct ways to proceed. Just to clear the matter with an example: Can police, in the absence of any judicial warrant, proceed to search the smartphone or another analogous device of a person upon arrest, an operation that usually is permitted by national legislations with regard to the traditional, real (instead of virtual) investigations? Or, as decided by the US Supreme Court in *Riley*, should they wait until a judicial authority allows them to proceed? [6].

As not enough, digital evidence and devices also present new problematic features concerning cooperation among judicial as well as administrative authorities. Data can indeed be contained not only in a variety of devices, either under the control of the offender or in the hands of third parties. They can even be stored in service providers located in jurisdictions other than the one where the proceedings are taking place. The transnational nature of these crimes – reinforced by the effects produced by market globalization – entails an improved need for judicial cooperation, because the data necessary to prove the facts may be, at least in part, located abroad [7]. At the same time, financial crimes, and first of all tax and

---

[4] See *supra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics: a comparative perspective*, § 6.

[5] See *infra*, under § 2.2.c.

[6] See under this aspect the famous decision of the US Supreme Court Riley v. California, 573 U.S. __ (2014). See G. Lasagni, *Tackling phone searches in Italy and in the US. Proposals for a technological re-thinking of procedural rights and freedoms*, in *New Journal of European Criminal Law*, Vol. 9 (2018), i. 3, p. 386 ff.

[7] See P. De Hert-C. Parlar-J. Thumfart, *Legal arguments used in courts regarding territoriality and cross-border production orders: From Yahoo Belgium to*

customs crimes, may easily require a form of "diagonal" cooperation [8], among the various law enforcement authorities, since one illicit behavior may easily constitute both a crime and an administrative offence, over which an enforcement agency other than the judiciary has jurisdiction. This is why, traditionally, financial crimes oblige various governmental administrations to work in connection with police and the judiciary, to reconstruct a full picture of the offence and to enforce the law at the best of its potentials.

The research conducted in this project confirmed these starting points. The reports on national jurisdictions referred indeed that fighting against such typology of crimes implies very often the involvement of various public agencies, required to cooperate for the better outcome of law enforcement purposes [9]. This may give rise, sometimes, to issues on the admissibility of evidence, because the legal requirements to present and admit evidence in criminal proceedings may be different from the standards provided by the law in administrative proceedings (even where bearing punitive purposes) [10]. Furthermore, from the national reports also emerges the recurring need to trigger mechanisms of judicial cooperation.

Finally, although focused mainly on financial and fiscal crimes (especially VAT offences), the research has confirmed that the management of electronic evidence (and its evolution, represented by the use of artificial intelligence systems – AI – and machine learning systems – ML), from its collection during the investigation up to its assessment at the end of the trial, is and will be one of the main challenges for the fair administration of criminal proceedings.

Microsoft Ireland, in *New Journal of European Criminal Law*, Vol. 9 (2018), i. 3, p. 326 ff.

[8] J. VERVAELE -A. KLIP, *European cooperation between tax, customs and judicial authorities: The Netherlands, England, and Wales, France and Germany*, Kluwer Academic Publishers, The Hague, 2002, p. 4; S. TESORIERO, *La cooperazione transnazionale nelle indagini in materia di frodi IVA e doganali: strumenti tradizionali e nuove opportunità*, in M. CAIANIELLO-A. DI PIETRO (eds), *Indagini penali e amministrative in materia di frodi IVA e doganali. L'impatto dell'European Investigation Order sulla cooperazione transnazionale*, Cacucci, Bari, 2016, p. 44 ff.

[9] F GIUFFRIDA-K LIGETI, *Admissibility of OLAF Final Reports as Evidence in Criminal Proceedings*, 2019, University of Luxembourg.

[10] Under this aspect, however, the answers received from the national reports are not homogeneous: see *infra*, under § 3.

2. *Results emerging from the research project*

2.1. *Common Solutions*

The research showed that the countries involved faced some common problems and under certain aspects dealt with them in a similar way.

2.1.1. *Starting from searches and seizures*

One first aspect worth mentioning concerns the assimilation of electronic investigative operations, aimed to gather data and use them in criminal proceedings, to searches and seizures. Generally, this occurred in the initial cases decided by the (national) courts, before the legislator intervened to adapt the relevant legal provisions to the new challenges brought about by electronic evidence. In practice, in all involved national jurisdictions, such cases were decided applying the rules concerning searches and seizures, perceived as the most proximate to deal with the new matters in question. This outcome may be easily understood. After all, browsing a device, with the aim to find information that is material to the case under investigation, may indeed seem analogous to searching a private premise: in both cases there is an expectation of privacy by the person whose premises (no matter if real or virtual) are searched and seized; in both cases, furthermore, the state of the places subject to search is usually altered at the end of the operations. Finally, in both cases the person whose property (no matter if real or virtual) was seized by the public authority has a legitimate standing to request its return, and to challenge the legality and the proportionality of the operation conducted (as well as of the orders issued by the judiciary authorizing the intrusion in the private sphere as such).

However, the common conclusion emerging from the national reports is that, in the long term, the provisions concerning traditional searches and seizures may be used to regulate new digital investigations only to a limited extent [11].

On the one hand, certain operations enabled by new software –

[11] See *supra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics*, cit., § 2.

such as malware or spyware – permit police to conduct operations unbeknownst to the defense, who may remain unaware for a long time of the occurred intrusion (even until the end of the investigations). Furthermore, the assimilation to old style searches and seizures does not work well with regard to the restitution of seized property when it comes to digital data, considering that the latter can be indefinitely copied and reproduced [12]. In digital investigations, moreover, seizure quite often antecedes the search: in fact, police usually first freezes the targeted device, so to preserve all the data contained in it, and then proceeds to make a copy of the entire system. After this, once the availability of all data potentially material to the case is secured, law enforcement carries out the opportune searches within the cloned copy, so to find what is specifically relevant to prove the case concerned by the investigation.

On the other hand, and most of all, digital instruments allow for investigative operations that are very different from any form of traditional search or seizure, and that can hardly be compared to analogous actions performed outside the virtual world. Investigative operations such as GPS surveillance, or the search for the identity of the owners of SIM cards or IMSI numbers [13], the monitoring of private conversations and correspondence, the activation of cameras or audio-recording instruments of the device thanks to new highly intrusive software, present characters that only in very general terms can be assimilated to analogue operations [14].

Therefore, we find another common exigency, emerging from the national reports: To amend the legislation concerning digital investigations following certain general criteria, such as technical neutrality; a rigorous proportionality control before and after the digital intrusion has been authorized; and an all-encompassing view of digital surveillance.

---

[12] See L. BARTOLI, *Sequestro di dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. pen. (web)*, 2018, i. 1, p. 1 ff.

[13] See A. CAMON, *Il cacciatore di IMSI*, in *Arch. pen. (web)*, 2020, i. 1, p. 1 ff.

[14] As the US Supreme Court observed in Riley v. California «Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom». See G. LASAGNI, *Tackling phone searches in Italy and in the US*, cit., p. 387.

2.1.2. *Technical neutrality in legislation*

The quest for digital neutrality in legislation is justified by the fact that digital devices present very short periods of technological obsolescence. On the opposite, legislation is designed to last over time, so that interpreters, first of all the courts, can develop uniform and stable interpretations that make the system predictable from the perspective of the individuals. A legislation that is focused too specifically on certain kinds of intrusive investigative techniques, allowed by the current developments of digital technology, would most probably risk being in very short time overtaken by new scientific or technological advancements.

Digital neutrality, however, may imply a problematic side effect, that is constituted by a certain margin of legislative imprecision. Just because of the need to avoid (a too fast) obsolescence of legal products, legislators sometimes tend to avoid narrow definitions in legal provisions dealing with electronic investigations, and this may give raise to some problems with respect of the principle of legality.

2.1.3. *The proportionality principle*

Proportionality control is generally provided for in all the examined countries. This is due to the fact that all the basic laws of the national jurisdictions involved, as well as the supranational European sources, provide for such rule, either explicitly or implicitly. While Germany and Spain enshrine proportionality in their respective constitutions, Luxembourg, the Netherlands and Italy provide for it in their legislation (and, in certain cases, the interpreters have implicitly derived this principle from the provisions of their respective constitutions) [15].

The increasing impact of European sources – both the ECHR and the EU sources – is contributing to give reinforced authority to the principle at stake. In sum, a proportionality check is needed in all examined national jurisdiction. Of course, the way in which the control is carried out differs, as well as the consequences attached to the disregard for what proportionality requires. For example, in certain systems the violation of the safeguard at stake may easily

[15] Analyzed in more detail *supra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics*, cit., § 2.

lead to the exclusion of the evidence collected, while in others such an outcome is very infrequent, if not at all absent. Anyway, the common idea remains, that that less intrusive investigative methods or instruments should be used if they can reach equal results, and that an impartial and independent authority needs to be empowered with the task of reviewing the proportionality of the investigative measure adopted.

2.1.4. *A comprehensive approach to digital investigations*

From national reports two opposite tendencies emerged in this regard. On the one side, that a limited and sectorial regulation of electronic evidence, focused only on certain aspects, and leaving the others to the provisions already in force for the traditional investigations, is an option definitely far from optimal [16]. On the other, however, that to intervene only in a circumscribed and sectorial way constitutes an easy and recurring temptation for national legislators. Having this perspective in mind, the outcomes of the conducted research showed that, prevailingly, States tend to find a certain level of compromise between the two alternatives previously depicted. The first to emerge is a tendency to deal with the collection of electronic evidence applying the legal provisions in force for the older non-technological investigations. This attitude may concern early legislative reforms enacted to regulate the matter: We could define this first phase as "Step 1". Subsequently, however, this approach gets reconsidered, and new normative solutions are elaborated to implement an autonomous concept and a consistent regulation of digital evidence – either thanks to new legislation or to an innovative jurisprudence of the Supreme Courts (we could call this following stage "Step 2").

Currently, examined States are prevailingly trying to follow the path described in Step 2 (not without troubles and inconsistencies) [17]. There are numerous reasons why this evolution oriented to elaborate an independent legal approach to digital

[16] Especially when it comes to defence and fair trial rights: see *supra*, L. BARTOLI-G. LASAGNI, *Antifraud investigations and digital forensics*, cit., § 6.

[17] The only exception seems to be represented by Italy where the debate, and the recent legal reforms, concerned only interceptions of communications, although conducted using new intrusive malwares or spywares. See *supra,* L. BARTOLI-G. LASAGNI, *Antifraud investigations and digital forensics*, cit., § 2.

forensics seems understandable, and should be sustained. As previously observed, the level of intrusion allowed by new digital tools of surveillance, no matter if concerning real time operations, or browsing and searching data stored in a personal device (or in cloud providers), is almost in every case incomparably higher than in traditional operations, because of the capacity of interfering with privacy and collecting a massive set of data crucial to reconstruct the entire identity of the person involved, in a lot of sensitive aspects. Distinguishing each form of intrusion permitted by the various forms of digital investigative operations, and creating different criteria and diverse legal standards for each of them, risks to produce, as a general result, an inadequate level of protection for individual rights, especially with regard to private and family life and to the protection of personal data [18].

Strong interferences with private life and the core area of individual personality, may indeed arise from any form of investigation performed on modern devices, such as bank surveillance, smartphone searches, the collection of personal data obtained by making a virtual copy of a personal device or online searches (without forgetting live surveillance allowed by the activation of malwares and spywares). This is probably why the jurisdictions whose legislation is more recent – certainly Spain, but also Luxembourg, Netherlands and Germany – have all tried to introduce a more comprehensive approach, here depicted as Step 2. National legislator thus showed an increased awareness of the implications caused by the so-called second digital revolution in the field of criminal investigations methods and operations [19].

On the opposite, the Italian legislator kept an approach strongly influenced by the past, trying to fit new digital investigations into

[18] See under this aspect the problem represented by what Quattrocolo defines as "investigative hacking", a concept that can adapt to a panoply of interferences by law enforcement agencies with private aspects of individual life. See S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Springer, Cham, 2020, p. 62.

[19] However, it must be recognized that these legislations, although oriented towards the autonomous and all-inclusive approach mentioned above, are in some respects incomplete and limited. For example, they rarely provide for specific remedies for violations occurred during digital investigations, or do not provide for specific right to be heard, or exclusionary rules. In other words, if we put together the pieces of the legislation of the various states, an almost comprehensive, but never really complete, regulation comes out. See under this aspect L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics*, cit., § 6.

old forms of "investigative operations concerning physical objects. This is perhaps due to the fact that the Italian normative provisions introduced to implement the Budapest Convention date back to 2008, at the very beginning of the new digital age, when Government and policymakers did not perceive in full the potentialities given by the new electronic tools, and have not since then been systematically reformed? [20].

No matter what provided by legislation, it is worth to outline that some relevant policies are however common in the examined Member States, for instance the choice of entrusting the processing of digital evidence to law enforcement bodies with a certain level of specialization. This option concerns mostly the phase of digital data analysis, while inconsistencies affect the solutions adopted with regard to the first steps of digital investigations (when the so-called First Responders come into action) [21]. Furthermore, this common policy choice does not as well open the path to common practices, which remain rather diverging [22].

2.1.5. *The need for more uniformity in the European realm*

Finally, another common aspect emerging from national reports is the desire for increased uniformity in legislation, both within national jurisdiction and at the supranational level. One of the common needs expressed in country reports is, in fact, that EU legislation should be adopted to harmonise domestic law and elaborate common standards in this field.

This final aspect is certainly related to the others previously

---

[20] It is regrettable, however, that in recent reforms enacted between 2017 and 2020, the Italian legislator has not reconsidered this approach. In fact, it has remained too focused on a single investigative tool, interception, without dedicating due care to other investigative operations made possible by technological development.

[21] See *supra,* L. BARTOLI-G. LASAGNI, *Antifraud investigations and digital forensics*, cit., § 4.

[22] For example, with regard to the specialization of investigative bodies, there is a lack of uniformity in the identification of the cases and use of specialised police units. The same holds true with respect to the definition of which (certified) competences these units should have to carry out digital surveys. Finally, the lack of a uniform approach regards the training for the so called First Responders. See *supra,* L. BARTOLI-G. LASAGNI, *Antifraud investigations and digital forensics*, cit., § 5-6.

mentioned. Uniformity and comprehensiveness constitute the golden thread of the matter. Uniform standards are indeed necessary both within each single jurisdiction, and at supranational level. With regard to the former, they are required to allow a consistent application of the provision concerning the gathering and use of e-evidence in administrative and criminal proceedings (diagonal cooperation). In relation to the latter, harmonized and all-inclusive provisions should be crucial to improve judicial cooperation and to ensure mutual recognition in the field of digital evidence (as well as to favor its admissibility, once the e-evidence is delivered in the jurisdiction where the proceedings take place).

2.2 *Diverging aspects*

The research conducted showed that, among the national systems taken into exam, there are numerous diverging aspects, that as such may give rise to some difficulties in pursuing an increased uniformity of legislations.

2.2.1. *National constitutional principles v. Supranational European principles*

The first troublesome discrepancy worth to be outlined, in the perspective of strengthening uniformity among legislations, concerns the role played in each jurisdiction by the principles contained in the respective constitutional provisions, read in relation with the European sources.

Two options seem at the antipodes. Germany, on the one hand, shows extreme care for its basic norms, although at the same time tends to give little or no relevance to the European sources coming from the treaties; in The Netherlands, on the other, a direct application of the national Constitution is prevented by the courts, while the opposite holds true for the European sources. Italy, Spain and Luxembourg are somehow placed in the middle, even if with different features and diverging nuances in the way in which their Supreme Courts are in dialogue with the European Courts. This aspect seems intertwined with the lack of a more uniform legislation at European level. It seems most probable that the different weight given to European principles in state jurisdictions has repercussions on the difficulty of adopting more uniform legislation at supranational level.

2.2.2. *Regulation in "criministrative" proceedings*

The first feature worth to mention concerns the regulation of procedures regarding administrative offences with punitive features. Here divergencies regard the full and uniform implementation of the *Engel* criteria. For example, the Italian system implements only in part the doctrine of "*matière pénale*" in its administrative legislation, not acknowledging in full certain basic fair trial rights, such as the right to silence and the right to an oral contest on equal footing between the defense and the investigating authority. Again, with reference to Italy, administrative rules of evidence barely respect the right to examine or cross-examine witnesses, that, on the contrary, is fully recognized in criminal proceedings *stricto sensu* [23]. In Spain, on the other side, the procedural implications of the *Engel* criteria are applied in a broader manner. The rules in fact prescribe a rigorous proportionality control and provide for a general exclusionary rule – with regard to evidence – also in the field of administrative law with punitive features. The same holds true for the Netherlands, where the principle elaborated by the ECtHR are applied, being as said before, the ECHR a source directly invokable by the parties in court [24].

Again, with regard to the procedure followed in administrative offences, discrepancies among States may be found in the general principles of the law of evidence. In Spain, for what is not explicitly regulated in the law, reference is made to the provisions of the code of civil procedure: This is consistent with its tradition, although such option leaves without appropriate regulation some aspects related to the management of electronic evidence [25]. In the Italian system too to the provisions of the code of civil procedure are applicable when the case is not specifically regulated, a choice that, however, is both inconsistent with its current legal framework, and inadequate to the management of the variety of problems regarding digital evidence. In other countries, like Germany, the law refers, if an *ad hoc* normative provision is lacking, to the code of criminal procedure.

[23] As it is well known, Italy is perhaps the country that, more than any others, in the European Continent (and possibly within the EU Member States), implements the orality principle and the right to confrontation in criminal proceedings.

[24] See *supra*, at § 2.2.1.

[25] According to the national report, the 2015 reform that provided the Spanish system with a clear and detailed legal framework on digital investigations and electronic evidence, is applicable only to criminal proceedings.

Luxembourg regulation seems to be situated somehow in the middle, because, on the one hand, it remands to the code of criminal procedure for what is left unresolved by the their specific provisions, while, on the other, the 2014 reform enacted to order the matter of e-evidence applies only to criminal case strictly defined, and not to administrative offences with punitive features.

Finally, the transfer of information and of the e-evidence from administrative to criminal proceedings is treated differently. Certain systems apply a rigorous check to ascertain that the fundamental safeguards of criminal justice are respected (this is what happens especially in Spain, and, under certain important aspects, in Germany and Luxembourg); others (such as Italy and the Netherlands) are more lenient, tending to admit any evidence coming from administrative authorities.

2.2.3. *Diverging features in the law of evidence*

From the above considerations, it emerges quite clearly that, probably, the most relevant difference among national jurisdictions concerns the way in which evidence is treated and, if necessary, excluded from the proceedings. This is not surprising *per se*, being the law of evidence by tradition highly diverging from one jurisdiction to another [26]: With regard to e-evidence, though, this may cause serious problems for judicial cooperation.

Firstly, one clear diverging aspect concerns the presence of provisions on exclusionary rules, as well as their application by domestic courts. This kind of normative reaction to procedural flaws occurred in the collection of evidence is recognized in some countries, such as Spain, Italy, Luxembourg and Germany, while is absent – in practice, if not in paper – in the Netherlands. Of course, big differences emerge in the way the exclusion of evidence is issued. Certain countries indeed require the applicant to raise the motion to suppress evidence at the earliest possible moment (Germany, for certain cases, and Luxembourg, where any evidentiary issue must be decided before the beginning of the trial); in others, on the contrary (Spain and Italy), judges may retain the power to

[26] On exclusionary rules as potential remedy see *supra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics*, cit., § 6.3.

exclude the evidence until the end of the trial (including, in this concept, the appeal phase).

Some similarities emerge instead with regard to the assessment of the evidence collected. National courts tend indeed to treat rather consistently the problem of e-evidence reliability, when some mismanagement occurred during its collection or preservation. Courts are in fact prevailingly reluctant to exclude e-evidence presented at trial because of mistakes occurred in the chain of custody. On the contrary, they usually prefer to tackle the issue within the final assessment of all information at the end of the trial. Said it differently, the uncertainty regarding the authenticity or the integrity of the data due to some mistakes committed in the collection, conservation or treatment of e-evidence, is prevailingly resolved by attaching a lesser evidentiary value to it.

2.2.4. *Legal provisions concerning documentation of digital investigative operations*

Another diverging aspect relates to the way in which law enforcement agencies document their operations when collecting, storing, treating and presenting digital data in criminal proceedings. While a certain convergence appears in the best practices, the opposite is true with regard to the legal provisions regulating the documentation of the various digital investigative operations [27].

Certain countries stick to the old "*procès verbal*", an option that looks really hardly apt to face the challenges represented by the multiple forms and the technical implications of digital investigations. Even though some scholars have longtime suggested videorecording as the best way to document rigorously every passage of the virtual operations [28], this option is not considered in

---

[27] On best practices in the national jurisdictions taken into consideration see *supra*, R. BRIGHI-M. FERRAZZANO, *Digital Forensics: Best Practices and Perspectives*, § 3.

[28] The reference goes, firstly, to the COE *Electronic Evidence Guide* (hereinafter "EEG"), which addresses the need of law enforcement and judicial authorities to acquire basic technical knowledge on what digital information and digital devices are, as well on which are the best practices to correctly handle digital technology at the crime scene. According to § 7.1, recording where the digital device was found and seized is important «because it can reveal a great deal about the intent of the suspected offender. It is good practice to record the search and seizure by video. This will show the position of digital devices, so that there is no longer an

any of the examined jurisdictions. Only the Netherlands law seems to provide for some form of recording of the digital operations, while probably the most innovative solution was enacted by the Spanish legislator, that assigned with new powers and responsibilities the judicial notary, a figure that is not recognized in any other national system considered in the current research [29].

The problematic aspect of the reported inconsistencies in documentation among States may be expressed in few considerations: On the one hand, legal provisions concerning documentation are different in every jurisdiction (and this confirms the need for more uniformity, as previously pointed out). On the other, the rules in force seem to disregard the new pitfalls that characterize the conduct of digital investigations. In particular, the problem of traceability and controllability of any data, to test its authenticity and reliability, appears prevailingly underestimated (with the exception of Spain).

Apart from the right to take part to the investigative operations performed by the police and the prosecutor, which must be granted when it is feasible, the only possible way to verify the correctness of the operations of the law enforcement agencies relies on the documentation of the investigations conducted. The more the documentation is accurate and precise, the more parties, and above all the defense, will be put in the position to raise issues with regard to the authenticity and the reliability of the information collected and presented. Inevitably, if the documentation is defective or inaccurate (or overly summary), courts will tend to be lenient in dealing with procedural flaws concerning the evidence involved: Simply said, in such circumstances there are not enough arguments to support more rigorous options.

---

argument, for instance, as to whether the wireless device was found hidden in the loft rather than in an open access area in the sitting room». An analogous option was proposed by some scholars with regard to genetic investigations. See A. Camon, *La disciplina delle indagini genetiche*, in *Cass. pen.*, 2014, p. 1431; F. Caprioli, *La scienza "cattiva maestra": le insidie della prova scientifica nel processo penale*, in *Cass. pen.*, 2008, p. 3530.

[29] See *supra*, L. Bartoli-G. Lasagni, *Antifraud investigations and digital forensics*, cit., § 6.2.

2.2.5. *The authority empowered to issue the intrusion in the private sphere of the individual*

Finally, with regard to the gathering of evidence, divergences concern the authority empowered to authorize the intrusion in the private sphere of the individual [30]. While the majority of the countries show a clear preference for a judicial intervention, when privacy and intimacy is at stake, certain countries still leave relevant powers to the prosecutor. This is the case of Italy, where this magistrate can issue any order concerning searches and seizures, included those implying the performing of digital investigations. The Netherlands too leaves a relevant power to the prosecutor, and the same holds true for Luxembourg, where this figure may issue freezing orders and shows some relevant evidentiary powers in crimes of milder gravity (the so called *délits*). At the same time, there is a lack of uniformity with regard to defence rights, concerning, for example, the modalities of participation of the defendant in the digital investigation, or in the design of remedies in cases of violation (this issue concerns both the problem of exclusionary rules and the right to appeal against improper intrusions occurred).

3. *Conclusions. The need for more uniform legal provisions to ensure effectivity both in law enforcement and fair trial rights*

The considerations made so far show that an increased uniformity in legislation, in the matters considered by the current research, would be most probably very helpful. Consistency in legal provisions concerning the collection, the treatment and the admission at trial of electronic evidence is necessary, as said before, both within national jurisdictions and at the supranational level.

On the one hand, in fact, harmonization would help domestic cooperation between authorities governing administrative proceedings on offences with punitive features (the so called *criministrative* justice) and judicial authorities competent to deal with criminal proceedings *stricto sensu*. On the other, it would

[30] See about subject K. KREMENS, *The authority to order search in a comparative perspective: a call for judicial oversight*, in *Rev. Bras. de Direito Processual Pen.*, 2020, v. 6, n. 3, p. 1585 ff.

improve judicial cooperation and mutual recognition within the EU Area of Freedom, Security and Justice, favoring the collection of digital data and their admission at trial at the translational level. We cannot forget, in fact, that the most part of the investigative operations involving digital devices are regulated, in the Directive on the European Investigations Order (2014/41/EU), under Chapter IV concerning «specific provisions for certain investigative measures». This Chapter provides, with few exceptions, for a double national check [31] (a legality control by the judiciary both in the issuing and in the executing State), in addition to the proportionality check. Diverging provisions may therefore represent an unsurmountable obstacle for effective cooperation, because an investigative measure issued in one State may not be considered legal in the executing jurisdiction. A legislative action aimed to harmonize safeguards and procedures in the field of evidence collected from, or, in any way, involving digital devices, would be most probably helpful. It would – last but not least – discourage the practice of forum shopping, whose attractivity, as well-known [32], increases the more national provisions are diverging and conflicting.

Once acknowledged the need for a more uniform regulation, one may wonder how this legislation should be shaped.

First of all, it needs to be said again that such harmonization should involve both administrative and criminal proceedings, because of the frequent transfer of information from administrative to criminal proceedings and vice versa.

Secondly, legal provisions should be inspired by the aim to be neutral from a technical perspective, so to avoid, for what is possible, risks of an early obsolescence.

Thirdly, legislation on e-evidence should bear a comprehensive vision to the matter of digital investigations, considering that any form of intrusion capable of collecting a critical mass of data needs to be regulated with the highest level of protection, according to the principles provided in the Treaties, the Charter as well as in the ECHR and its case law.

---

[31] J. Vervaele, *European Investigation Order and financial investigations in The Netherlands*, in M. Caianiello-A. Di Pietro (eds), *Indagini penali e amministrative in materia di frodi Iva e doganali*, cit., p. 383.

[32] See M. Böse, *Choice of Forum and Jurisdiction*, in M. Luchtmann (ed), *Choice of Forum in Cooperation Against EU Financial Crime*, Eleven, Den Haag, 2012, p. 73.

Fourthly, normative provisions should require a judicial control both before and after the collection of data (or, in any case, attribute the power to approve the intrusion on the individual private sphere to an authority that ensures the same level of independence and impartiality given by a judge).

Finally, legislation should require an accurate documentation of the operations conducted by police, prosecutors and other law enforcement agencies, so to provide the parties, first of all the defense, with a complete traceability of the chain of custody.

As previously said the main challenge to the fair administration of criminal (and *criministrative*) proceedings concerns and will continue to concern the management of e-evidence. This task is going to be even more important with the spreading of Artificial intelligence and Machine Learning systems, intended to help the judiciary as well as other adjudicative authorities in the administration of justice. The trend oriented to use immense amount of data located in the virtual sphere, related to the private domain of any individual, is exponentially increasing [33].

Finding a way to submitting digital evidence to the Socratic method, so as to allow parties to have adequate legal instruments for cross-validation of the collected digital information, constitutes indeed the ultimate challenge to preserve the traditional pillars on which modern criminal proceedings are founded [34], and to "translate" them in the new realm generated by the second digital revolution [35]. Failure in this feat may lead to a huge transformation of the nature of criminal proceedings that may become an instrument used much more to prevent future crimes than to reconstruct facts of the past.

Under this aspect, it seems at all not surprising that, the more e-evidence and automated system are introduced in criminal

---

[33] S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 16.

[34] As "traditional pillars", I am firstly referring to the retrospective nature of fact-finding in criminal trials, the dialectic method characterizing the way in which evidence is presented, the criterion of reasonable doubt that the judge needs to apply in adjudicating. See M. CAIANIELLO, *Criminal Process faced with the Challenges of Scientific and Technological Development*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2019, p. 265.

[35] See M. WASHINGTON-N. RICHARDS, *Digital Civil Liberties and the Translation Problem*, in *The Oxford Handbook of Criminal Process*, D. K. BROWN-J.I. TURNER-B. WEISSER (eds), Oxford University Press, Oxford, 2019, p. 365-391.

proceedings, the more the pressure to use criminal proceedings for preventive rather than repressive purposes is increasing [36]. Criminal proceedings have always been an instrument of social control. However, as long as they maintain a retrospective function, focused on past events, their effectiveness as a tool for controlling human behavior is limited. The massive use of digital evidence – if not administered properly and if not rigorously and scrupulously submitted to the basic principles of modern fair trials – may favor the transformation of criminal proceedings in their essential nature, hugely affecting rights and freedoms achieved in the last three centuries by democratic societies. If we want to safeguard the principles that have characterized the administration of criminal justice in the post-Enlightenment period, now is the time to intervene, reconciling the great opportunities that new digital age opens up with the new, and no less significant, dangers that it may imply.

[36] On the difference between predictive policing and predictive justice, that open the path to the turn of criminal justice to a system of preventive justice, see S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, cit., p. 39.

CONTRIBUTORS

Lorena Bachmaier Winter
DEVICES' Legal Expert for Spain
Full Professor of Law – Universidad Complutense de Madrid

Laura Bartoli
DEVICES' Junior Staff member
Postdoc researcher – University of Macerata

Raffaella Brighi
DEVICES' Senior Staff member
Associate Professor of ICT&Law – University of Bologna

Michele Caianiello
DEVICES' Senior Staff member
Full Professor of Criminal Procedure – University of Bologna

Alberto Camon
DEVICES' Coordinator
Full Professor of Criminal Procedure – University of Bologna

Michele Ferrazzano
DEVICES' Digital Forensics-Expert
Postdoc Researcher – University of Modena and Reggio Emilia

Sabine Gless
DEVICES' Legal Expert for Germany

Full Professor of Criminal Law and Criminal Procedure – University of Basel

GIULIA LASAGNI
DEVICES' Junior Staff member
Postdoc Researcher-Adjoint Professor – University of Bologna

KATALIN LIGETI
DEVICES' Legal Expert for Luxembourg
Full Professor of Law – University of Luxembourg

GAVIN ROBINSON
DEVICES' Legal expert for Luxembourg
Postdoc researcher – University of Luxembourg

THOMAS WAHL
DEVICES' Legal Expert for Germany
Senior Researcher at the Max Planck Institute for the Study of Crime, Security and Law

In this series

1. AA.VV., *Legge e potere nel processo penale. Pensando a Massimo Nobili* (atti del convegno, Bologna, 4 e 5 novembre 2016), 2017, p. VIII-255
2. MARCELLO L. BUSETTO, *Controlli giudiziali sulla qualità della difesa tecnica. Un itinerario fra fonti europee e diritto interno*, 2017, p. VII-239
3. VALENTINA BONINI, *Il sistema di protezione della vittima e i suoi riflessi sulla libertà personale*, 2018, p. IX-434
4. DANIELE NEGRI e LORENZO ZILLETTI (a cura di), *Nei limiti della costituzione. Il codice repubblicano e il processo penale contemporaneo*, 2019, p. XV-321
5. FABIO NICOLICCHIA, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, 2020, p. XIII-246
6. LAURA BARTOLI, *La sospensione del procedimento con messa alla prova*, 2020, p. IX-474
7. MICHELE CAIANIELLO and ALBERTO CAMON (edited by), *Digital forensic evidence. Towards common european standards in antifraud administrative and criminal investigations*, 2021, p. 1-170