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.