How a Standardization Process May Impact on the Relation Between Digital Evidence and Digital Forensics

Stoykova, Adi

Published in:
Jusletter IT

Publication date:
2018

HOW A STANDARDIZATION PROCESS MAY IMPACT THE RELATION BETWEEN DIGITAL EVIDENCE AND DIGITAL FORENSICS?

Radina Stoykova

Ph.D. researcher, ESSENTIAL project: essentialresearch.eu, ITTIG-CNR Italy
Institute of Legal Information Theory and Techniques, Italian National Research Council
Via de' Barucci 20, 50127 Florence, IT
radina.stoykova@ittig.cnr.it

Keywords: ***standardization, digital forensics, digital evidence***

Abstract: *Legal, technical and scientific standardization is presented as complementary approach to the CoE and EU legal initiatives to improve cross-border exchange of digital evidence. Policy-making for digital evidence is considered as a network of standards between different stake-holders (forensics specialists, law enforcement and service providers), which can be equally sound in law-making, court proceedings and forensic science, because it would provide a basis to guide or interpret legal fact-finding, but it would also have the flexibility to adjust to specific jurisdictions, other legal domains, and technologies in an agile manner.*

1. Introduction

Digital devices in relation to criminal investigation can provide valuable evidence, but likewise pose a risk to the integrity of such evidence where data could be tampered, altered or manipulated, while inexperience and ignoring standard guidelines may result in data loss. This, and the divergent legal frameworks on handling digital evidence, pose a challenge to its admissibility and weight in court. To address the issue, both legal and forensic standards within each step of the evidence life cycle need to provide quality assurance, while requiring a holistic international approach of the framework governing criminal investigations. According to United Nations` report a "number of countries recommended that international standards should be developed on law enforcement investigations concerning extraterritorial data, including with a view to clarifying the relationship of such investigations with national sovereignty principles."[1] Therefore, it is important to examine the benefits and drawbacks of such standardization process.

2. Understanding of key terms

2.1 Digital evidence

Because digital evidence is not bound to territory and is always an abstraction of the computer intermediary[2], there are multiple specifics in its nature, types, life cycle and chain of custody. That is why it may be considerable to see it as a process – its probative value may depend not only on the evidence itself, but also on the associated metadata (say time and date stamps), the computer system's integrity and security (as source of the evidence), the consistency of the Digital Forensics (DF) methods (scientific evidence) and the preservation time (storage, technical obsolescence). Twenty years ago, the first model law initiatives[3] for international regulation of evidence were focused on adapting rules for "traditional" physical evidence to electronic evidence,

[1] UNODC, Comprehensive Study on Cybercrime, Draft—February 2013.
[2] CASEY, EOGHAN, Digital Evidence and Computer Crime, Third Edition, Elsevier, 2011, pp. 25: Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred. Furthermore, using a forensic tool to recover a deleted file from storage media involves several layers of abstraction; MASON, STEPHEN "Electronic evidence", 3rd edition, Lexis Nexis, 2012, pp. 30.
[3] HIPCAR, Electronic Evidence: Model Policy Guidelines & Legislative Texts, ITU, 2013.

but possibly with incomplete understanding of key concepts. Compared to more recent ones[4] it is notable, that the growing amount of digital evidence in criminal proceedings and evidence from foreign jurisdiction, shifted the focus to the electronic data specifics, requirements for admissibility, integrity through the whole chain of custody and evidence exchange models. In addition, jurisdictions are facing some similar issues in regards to digital data, which opens a dialog for a global standard governing digital evidence. *Mason* discusses possible models for Convention based on private initiative or non-binding initiative by way of regional fora or international agency[5]. The objective in this paper is to better understand possible implications of standardization, without proposing a legal model, but searching interlinks or gaps of law and forensics emergence in the evidence domain.

2.2 Digital forensics and quality assurance

Digital forensics[6] is the bridging discipline, which aligns technical capabilities with legal requirements in order to turn data into evidence. While the need of a standard scientific framework is widely recognized among digital forensic experts[7], its implementation in the legal and law-making process is still underdeveloped. Moreover, the cooperation between police authorities and American internet service providers (ISPs) is on voluntary basis and there are no specific legal requirements on what kind of data (i.e. subscription, transaction or content data), time limits and in which format will be provided[8]. In addition, judges understanding of the digital forensic methods and their quality is of great importance[9] in order to avoid either blindly accepting the digital forensic results, or on the contrary, disregard or lower the digital evidence's value.[10] The validation of the evidence, largely dependents on the skill and knowledge of investigators"[11]. However, judges or lawyers must evaluate their findings for how the evidence support the truth. Conceivably, the evidence domain purely legal approach will be insufficient, since legal, technical and scientific principles must complement and also constrain each other.

Back in 2011, the Council of EU established the European forensic science area (EFSA) and European Network of Forensic Science Institutes (ENFSI), and pointed to the lack of "any [internationally] recognised quality standards" for digital forensic processes and systems, and the lack of transparency[12] as a major problem. The potential of developing new standardization or mapping the existing one to the digital evidence specifics – not only scientifically or technically but also legally, in order to improve these processes, requires examination from a theoretical and practical point of view.

---

[4] MASON, STEPHEN, Draft Convention on Electronic Evidence, Digital Evidence and Electronic Signature Law Review, 13,2016; and The Commonwealth, Draft Model Law on Electronic Evidence

[5] MASON, STEPHEN, Towards a global law of electronic evidence? An exploratory essay, Amicus Curiae The Journal of the Society for Advanced Legal Studies, Issue 103, 2015.

[6] See DFRWS, 2001 definition: the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorised actions shown to be disruptive to planned operations. Or EVIDENCE PROJECT, D2.1 - SEMANTIC STRUCTURE, pp.85: Digital forensics is the application of forensic science to Electronic Evidence in a legal environment.

[7] See COHEN/ LOWRIE/ PRESTON, 2011; CASEY, 2004; Beebe/Clark, 2005.; MCKEMMISH, 1999, NIST, 2006, Ó CIARDHUÁIN, 2004, CARRIER & SPAFFORD, 2003, DANIEL, 2011 etc.

[8] COUNCIL OF EUROPEAN UNION Note 9543/17, Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace, Brussels, 22 May 2017.

[9] KESSLER, GARY, Judges' Awareness, Understanding, and Application of Digital Evidence, Doctoral dissertation, Nova Southeastern University, NSUWorks, Graduate School of Computer and Information Sciences.

[10] https://www.natlawreview.com/article/court-finds-google-earth-images-to-be-admissible-evidence; and BOWLES, TRACY, Remote Sensing and Geospatial Data Used as Evidence: A Survey of Caselaw, 2002 at: http://www.crowsey.com/pdf/caseLawSurvey.pdf .

[11] IBID., fn 9.

[12] EUROPEAN COUNCIL conclusions on the vision for European Forensic Science 2020, Brussels, 2011. Emphasises mine.

2.3 Standards as legal requirement

For this purpose, standards are understood as quality policies linking forensic science and evidence-related laws in approach to international harmonization, since such standards could establish sets of solutions and models to potentially matching problems. Or in the words of the European Council "minimum forensic science standards" must be complemented with a "***common approach*** to implementation of these standards that fosters closer cooperation between them and the criminal justice systems"[13]. A standardization process within the evidence domain, its benefits and drawbacks, are outlined in a legal, forensic (scientific) and technical context.

2.3.1 Theoretical background

Understanding the nature of legal standardization process is derived from Hart`s concept for the secondary rule of recognition, which aims to "remove the uncertainty of the regime of primary rules by providing a rule for conclusive identification of the primary rules of obligation" and "in terms of the more complex social situation where a secondary rule of recognition is accepted and used for the identification of primary rules of obligation"[14]. This process could be described as achieving regulatory goals by directly improving the technology and its link to scientific research in the emerging disciplines, related to the evidence domain.

Schum refers that the evidential foundation of probabilistic reasoning is based on several disciplines like law, philosophy, logic, semiotics, artificial Intelligence, psychology and history[15]. Moreover, *Twining* argues that some limitations and inconsistencies in the legal perception for evidence might be overcome in the light of examining basic interdisciplinary approaches to evidence like narrative, generalisations, and argumentation[16] Both studies explain the importance of a scientific approach to evidence, which in contemporary terms relates to the question how to convey the probative value of evidence in the forensic process. Further, "objections to rigid versions of 'evidence-based' policy-making is that an evidentiary perspective tends to gloss over the political, ideological, or ethical aspects of policy decisions".[17]

2.3.2 Potential drawbacks of a standardization process

When considering multiple types of evidence, the volume of data and fast changes in technologies with relevant effects on practitioners (i.e. digital forensic experts) - extended standardization may lead to information loss. Some insights regarding the negative impact of over-standardisation could be derived by analogy for certain aspects of cloud-computing[18] and the related proliferation of standards. Distort import of international standards may have negative impact on national criminal laws as examined in relation to international criminal procedures[19]. In addition, the studies on the use of comparative reasoning in court as a way to align procedures and create global common standards for criminal adjudication vary strongly –conclusions, that judges are insusceptible to external influences[20] contradict to arguments that foreign and international law is an effective instrument for empowering the domestic democratic processes[21]. Other limitations are related to the fact, that "formal consensus in standardization is often very slow".[22] Moreover, insufficient oversight and auditing may

---

[13] IBID., fn 11.
[14] HART, H.L.A., The Concept of Law, 3rd edition, 1961.
[15] SCHUM, DAVID, The Evidential Foundations of Probabilistic Reasoning, John Wiley & Sons, 1994.
[16] TWINING, WILLIAM, Evidence as a multi-disciplinary subject, Law, probability and risk, vol.2, 91-107,2003; and "Rethinking Evidence: Exploratory Essays", Cambridge University Press, 2nd edition, 2006.
[17] IBID., TWINING, on pp. 449.
[18] WALDEN, IAN/GLEESON, NIAMH, It's a jungle out there'?: Cloud computing, standards and the law", in European Journal of Law and Technology, Vol 5, No 2, 2014.
[19] ELBERLING, BJÖRN, "The Defendant in International Criminal Proceedings: Between Law and Historiography" Hart Publishing UK, 2012.
[20] BOBEK, MICHAL, Comparative Reasoning in European Supreme Courts: An Introduction, Oxford University Press, 2013.
[21] BENVENISTI, EYAL, Reclaiming Democracy: The Strategic Uses of Foreign and International Law by National Courts, American Journal of International Law, Vol. 102 (2), 2008, pp. 241-274.
[22] FARRELL, JOSEPH, Choosing the Rules for Formal Standardization, University of California, Berkeley, 1996, pp.4: "Cargill (1989, page 114) reports that reaching a standard takes \an average of four years to complete; much more, if [it is] controversial". Kolodziej

result in inconsistency and redundancy. The issue with proliferation of standards might be addressed with policies for standardization development, quality testing of quality procedures and methodology to avoid duplication or contradiction in existing standards. However, every standardization process must rely on or with time emerge in mandatory legislation, which encourages policies and best practices for cooperation in evidence exchange while sufficiently insuring sovereignty of all countries, enforcement and judicial supervision. In achieving this, a precondition will be "standards that are not prescriptive with respect to methodology, but recognise existing accepted practice and form an achievable, cohesive and consolidated quality and risk management benchmark for laboratory managers and accrediting bodies" [23].

Some argue, that there is no possibility to map minimum standards for evidence, since "evidence" is a legal construct, not a "real thing" and depends on courts (legal doctrine) understanding of it and on mutual trust".[24]

2.3.3 Potential benefits of a standardization process

On the contrary, in a cross disciplinary hypothesis digital evidence is not a purely legal construct, but interlinks the forensic science (DF specific solutions, methods and tools), technology (platforms and system to facilitate the chain of custody) and law (legal requirements for criminal evidence). The extraterritorial and crossdisciplinarity nature of digital evidence needs a specific approach, which can overcome jurisdiction obstacles while respect legal tradition, to increase the general admissibility of digital data as evidence.

Moreover, this regulative impact must be achieved in an emerging environment within the young discipline of digital forensics. *Abbott and Snidal*, who build upon *Koremenos's* work, argue that soft law realm opens when "legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation", and in international context "facilitates compromise between weak and powerful states", considering that "nonstate actors […] press for different forms of legalization"[25]. Considering the power nonstate actors like ISPs have over data, even with legal framework on evidence, there will be still the need of synchronizing their cooperation with state authorities. Particularly, in new legal environments, standards, unlike hard law, can "deal with uncertainty, especially when it initiates processes that allow actors to learn about the impact of agreements over time".

Consequently, standards are more flexible than legal rules, because they are based on multi-stakeholder consensus and can act globally. They contain best practices and policies, which can be used as supplements or substitutes to legal rules, have an important *ex ante* function, while criminal laws generally act *ex post* and could pave the way for more comprehensive, legislative initiatives or transpose already existing. In addition, standards have a distinct enforcement impact through auditing and certification and indirect impact on the process of implementing legal rules in/to future technology. Moreover, standardized processes in the chain of custody will ensure more trust among LEAs and judicial authorities from different countries, when exchanging evidence cross jurisdictions and cooperation, instead of competing investigations in trans-border crime.

In this sense, any practical solution must meet certain scientific, legal and technical standards, which should be soundly interlinked and internationally valid. Controversially, firstly large effort is put into scientific and technical solutions, while judicial cooperation and understanding as to how digital evidence support the truth and how to be challenged on solid grounds in court is insufficient. Secondly, the loose interlinking of the three factors is at the expense of its admissibility and probative value.

(1988) estimates four to five years as an average. In 1981 the chairman of the IEEE Standards Board cited seven years as an average delay for an IEEE standard (Lee, 1981)".

[23] ANZPAA NIFS - Deconvoluting Forensic Standards a Review – External Release – May 2016, para 72 and 73.

[24] GLESS, SABINE, Free movement of evidence in Europe, Eclan/ COLEX, 2006, pp.121-131.

[25] ABBOTT, KENNETH W./SNIDAL, DUNCAN, Hard and Soft Law in International Governance. International Organization, Vol. 54, 2000, pp. 421.

3. Legal standardization impact on forensics and evidence

Developing minimum standards for digital evidence and systems to facilitate their secure exchange was laid down in the Stockholm Programme back in 2009[26]. Earlier this year, EUROPOL identified as a pressing open issue the "establishment of a consolidated cooperation framework for the collection and exchange of evidence […which] should include relevant national and international stakeholders such as private industry, and to the extent possible follow a standardised approach"[27].

Two recent legal initiatives, the European Commission`s communication on EU level[28] and the proposition for second additional protocol to the Budapest convention on CoE level[29], based on the Recommendations of the Cloud evidence group[30], are dedicated to enable and improve the cross-border exchange of digital evidence. Proposed are three evidences exchange models: *1. improving of mutual legal assistance regime, 2. direct co-operation with ISPs through production orders/ requests and 3. direct access from seized computers, or remotely from investigators' machines*.

Notably, these initiatives focus on some purely legal shortcomings in the evidence process – like defining types of digital evidence, and of safeguards and rules to be followed in the different regimes, as well as tackling the "loss of location" issue by addressing the legal fragmentation and the conflicts of law, or enabling searches for evidence the location of which is unknown or volatile. A significant effect on forensic cooperation between LEAs from different MS will have the definition of "connecting factors", which is based on the type of data and regulates potential effects of online investigation measure on another country's territory.

Along with the addressed legal challenges, a strong call for practical solutions and standardized approaches is mapped. Particularly, efforts are focused in two directions: firstly, the *administrative standardization* – aligning the forms of requests, accelerating procedures, improving safeguards, authentication and enforcement mechanisms. Secondly, *technical facilitation* of evidence exchange by developing new platforms and connecting/ improving existing ones as examined in Part 5. Based on the legal documents, further some practical implications are discussed, bearing in mind that for now these are only propositions for legislation.

Considered are improved and faster mutual legal assistance (MLA) mechanisms to provide legal ground for remote and cloud forensics. Further measure is the facilitation of evidence exchange platform with robust security. Legal standards for ISPs forensic readiness complemented by standard channels and procedures for data exchange with LEAs, will also reduce the different approaches to evidence among private companies offering the same services. Another proposition for effective case management and workflow are dedicated SPOCs[31] (single point of contacts for cross-border law enforcement information exchange) and entry points on the ISPs side. However, most countries have SPOCs in compliance with Art. 35 Budapest convention requirement for 24/7 network. In addition, new regulation[32] require eu-LISA to develop a central monitoring capacity for data quality of large databases (e.g. SIS II, VIS, EURODAC, ESS[33]) and development of anonymised data warehouse with LEAs access to it on the principle hit-no-hit identification. The new ENISA

---

[26] EU COMMISSION, Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 2010.
[27] EUROJUST / EUROPOL 7021/17 "Common challenges in combating cybercrime", Brussels, 13 March 2017, pp.14.
[28] COUNCIL OF EUROPEAN UNION, Note 9543/17, Technical document: Measures to improve cross-border access to electronic evidence for criminal investigations following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace, Brussels, 22 May 2017.
[29] T-CY, Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, Strasbourg, 9 June 2017.
[30] CLOUD EVIDENCE GROUP Final report, "Criminal justice access to electronic evidence in the cloud".
[31] Presidency note 8433/17 Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, Brussels 11 May 2017.
[32] EU COMMISSION, Proposal for a Regulation on the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, and amending Regulation (EC) 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) 1077/2011 Brussels, COM (2017) 352 final on pp.7.
[33] EU databases under eu-Lisa control to which LEAs will also have access: second generation Schengen Information System (SIS II); Visa Information System (VIS); European Asylum Dactyloscopy Database; Entry-Exit System (EES).

regulation[34] provides for establishing a harmonised framework for security certification of IT products and service, and underlines the importance of consistency with certification mechanisms for data protection seals and marks for the purpose of demonstrating compliance with GDPR[35]. The non-exhaustive examples prove ongoing standardization approach with direct impact on digital evidence process.

Moreover, cross border exchange of evidence based on the European investigation order[36], which entered into force this year, challenges MS to find suitable solutions to approximate their laws and policies[37]. Particularly, standardization could be applied in regards to resolving issues in combining *lex loci* and *lex fori* to provide maximum flexibility for evidence exchange, time limits compliance and prioritisation of cases, criteria for refusal, practical measures for evidence gathering in real time. A comprehensive study on international evidence exchange concludes that certification can "indicate that the taking of the investigative measure is possible in a similar national case"[38]. These legal standardization efforts have dualistic impact – they will change administration and facilitation of digital evidence and forensics, but at the same time provide a chance for forensic specialist to map insights in international dialog for evidence exchange. For example, time limits and prioritization of cases could compliment efforts in law enforcement laboratories for case management, resource allocation and efficiency within organization as well as international cooperation. However, the ongoing initiatives are focused on effectiveness and more security in the evidence process, but give no answers how the legislator will achieve its goal for stronger cooperation between digital forensic specialists and criminal justice systems[39].

4. Scientific standardization process

Scientific standardization processes in digital forensics were acknowledged 10 years ago[40], and nowadays the forensic science principles[41] and methodology are applied to digital forensics in order to develop this new branch and ensure research and education corpora[42]. This impacts the efforts for creating a comprehensive international legal Framework for evidence at least in three important aspects. Firstly, digital forensic corpora with methodologies for tool verification, reproducibility of results and accuracy improve mutual legal assistance, admissibility and standardised probative value, but raise questions about the balance between practical and efficient technical solutions on one hand and human rights and civil liberties on the other. Secondly, the scientific approach of the pre-trial investigation gains more importance, while court proceedings are formal and inefficient, which reflects on the issue that experts are dominating the dispute resolution in court. Finally, the scientific standardization of digital forensics can ensure predictability and certainty in the analysis, but also to provide exact knowledge where a regulatory approach is needed.

Cohen argued that "scientific consensus in the area of digital forensic evidence examination is lacking in the broad sense, but that different groups within that overall community may have limited consensus around areas

---

[34] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), COM 477 final, Brussels, 2017.

[35] IBID., at "Consistency with other Union policies".

[36] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

[37] E.g. EIO Directive, Rec.24, Art.9 and Art. 14.

[38] VERMEULEN, G./DE BONDT, W./VAN DAMME, Y., EU cross-border gathering and use of evidence in criminal matters. Towards mutual recognition of investigative measures and free movement of evidence?, IRCP, vol.37, Maklu, 2010.

[39] See fn13.

[40] GARFINKEL, SIMSON/ FARRELL, PAUL/ ROUSSEV, VASSIL/ DINOLT, GEORGE, Bringing Science to Digital Forensics with Standardized Forensic Corpora, DFRWS USA, Montreal, Canada, 2009.

[41] CASEY, EOGHAN, Digital Evidence and Computer Crime, Third Edition, Elsevier, 2011 on pp.14: Forensic Science provides a large body of proven investigative techniques and methods for achieving the ends that are referenced extensively in this text. By forensic we mean a characteristic of evidence that satisfies its suitability for admission as fact and its ability to persuade based upon proof (or high statistical confidence).

[42] YANNIKOS, YORK/GRANER, LUKAS/ STEINEBACH, MARTIN/ WINTER, CHRISTIAN, Data Corpora for Digital Forensics Education and Research, 10th IFIP International Conference on Digital Forensics (DF), 2014, Vienna, Austria.

in which they have special expertise."[43] In terms of the legal developments in cross-border exchange of evidence, the mutual recognition principle in EU introduced with the EIO and the international movement towards system interoperability "the community needs to adopt standardized, modular approaches for data representation and forensic processing"[44] to move forward.

The legal initiatives for evidence cross-border exchange show that the scientific standardization will no longer be left at the discretion of forensic specialists, but will be enshrined in a larger and global legal standardization process. This follows from the EU Commission statement when referring to collection of evidence in cross-border cases, that there is a need of "minimum principles to facilitate the mutual admissibility of evidence between Member States, including scientific evidence."[45]. In US the Daubert`s principle[46] is also questioned for its practical use in the absence of "standard […] established and certified by the justice system" on the possible legal evaluation and challenging of forensic findings in court[47]. In UK the criticism on the presumption of reliability of computer systems, expose missing standards on quality, reliability and integrity of evidence, covered by incomplete understanding and application of the presumption[48]. In civil law systems either the same presumption exists[49] or specific rules on how in practice the probative value of digital evidence is evaluated are lacking[50]. However, the following comparison of legal and forensic analysis on reliability and authenticity of evidence, shows that all jurisdictions face some similar issues.

4.1 Legal questions in scientific standardization

Scientific evidence always has a degree of uncertainty[51], caused by either potential human error or data corruption. *Casey,* while examining the possible errors in digital evidence, concludes that "we should evaluate computer-generated records based on the reliability of the system and process that generated the records" and refers to *Strong*, who suggests that digital evidence must not be presented in court as expert testimony, but "admissibility should be determined on the basis of the reliability and accuracy of the process involved"[52]. Further *Teppler* argues to be handled as hearsay[53]. However, in court often computer system integrity is not even questioned[54] or challenged on "slender grounds"[55], or courts from both common and civil law systems relay on presumption of "reliability" of computer systems[56].

In US, the Daubert`s rule for expert scientific testimony requires validation of the method, error rate, scientific acknowledgment and independence, which is broadly recognized in academia and among practitioners from both the legal and the digital forensics domain. NIST contributed to standardization of the process for Computer Forensics Tool Testing (CFTT)[57], which consist of a specific methodology to demonstrate the reliability

---

[43] COHEN, FRED, Column: Putting the Science in Digital Forensics, Journal of Digital Forensics, Security and Law: Vol. 6(1) , Art.1, 2011.
[44] GARFINKEL, SIMSON, Digital Forensics Research: The Next 10 Years, Digital Investigation 7, Elsevier, 2010.
[45] EU COMMISSION, Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, COM/2009/0624 final.
[46] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
[47] MARSICO, CHRISTOPHER, Computer Evidence v. Daubert: The Coming Conflict, TECH 581G Semester Research Paper in Computer Forensics, 2004.
[48] MASON, STEPHEN, Electronic Evidence, 4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017, Chapter 6, 6.210 and 6.219.
[49] EVIDENCE PROJECT, D3.1, pp. 19 – regarding Romania, Portugal, Spain.
[50] IBID., Table 3, Responses to questions 8.
[51] CASEY, EOGHAN, Digital Evidence and Computer Crime, Third Edition, 2011 Elsevier, para 3.3.1 on pp.70.
[52] CASEY, EOGHAN, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2010.
[53] TEPPLER, STEVEN, Testable reliability: A modernized approach to ESI admissibility, Ave Maria Law Review, 2014.
[54] TAYLOR, M./ HAGGERTY, J./GRESTY, D./HEGARTY, R., "Digital evidence in cloud computing systems, Elsevier, 2010: In the case of R. v. Spiby [1991] (CLR, 1991) it was held that if an instrument (in this case a computer) was of a kind as to which it was common knowledge that they were more often than not in working order, in the absence of evidence to the contrary, the courts will presume that a mechanical instrument is in working order at the material time.
[55] IBID., MASON at 6.193.
[56] IBID.,fn 45 and 46.
[57] https://www.cftt.nist.gov/disk_imaging.htm.

of forensic results, to identify potential errors, and at the same time to support admissibility of evidence. However, a new issue emerged, when the need for sharing tool testing results and for cross-verifying them could not be fulfilled, since different labs used different formats for the reports. Alignment of the practices in standard reports allow this to be overcome[58]. Also in relation to data protection requirements, "data controllers holding information in a non-standard format to convert it into a standard one" was proposed as a solution for ensuring data subject rights[59]. It seems that legal requirements for evidence foster more scientific standardization, without however, considering if this will positively impact the traditional trial. More importantly, truth and accurate evidence is only one part of the judicial evaluation of a case, but other aspects like civil liberties, human rights (right to access to justice, right to fair trial, data protection) remain remote to the evidence process. Notably, scientific standardization can improve a lot the evidence chain of custody, but *per se* is insufficient, if not practically implementing also legal requirements.

Another example can illustrate the exponential complexity of scientific digital evidence, which call for more scientific knowledge by legal practitioners and forensic experts. Likelihood ratio (LR) gains importance when DF specialists present their findings in court, since there is a practical need of quantitative methods for presenting digital evidence analysis and related levels of certainty. In addition, knowing possible error rates in the methods of software, judges can estimate to what extend the scientific evidence is trustworthy. However, *Lund and Iyer* "find this likelihood ratio paradigm to be unsupported by arguments of Bayesian decision theory, which applies only to personal decision making and not to the transfer of information from an expert to a separate decision maker" (judge), because "computing an LR is generally not free from prior probability assignment at the level of specific scenarios"[60]. They propose a "lattice of assumptions" paradigm instead, to reveal the decision-making process by experts. Such discussions relate to the question when cross-testing and verification become impractical, if at stake are criminal charges. One can argue, whether at all this assessment should be done by forensic examiners and if a judge participation in this pri-trial phase is not a better solution. Others, refer to the danger of machine bias, discrimination algorithms and the lack of policy, endangering the very basis of society[61] - an issue well-known also in the data protection domain when it comes to automated decision-making. ENFSI in its action plan relates to "creating standards for interpretation of scientific evidence"[62]. Initiatives to promote reliability in the submission and handling of expert evidence, resulted in a Guide in statistical evidence for legal professionals[63].

4.2 Reliability and authenticity standard

Often both legal and forensic evaluation of the digital evidence depend on cross-verification of the accuracy of forensic results, tool testing, reproducing the results by other DF specialists and with other methods. However, the criteria and approach how to do this vary and depend on the way an evidence will be challenged in court, if at all challenged. *Mason*, refers to *Reed and Angel`s* two hypotheses[64] – either the computer system or software was not functioning properly and created evidence, that does not support the truth or although the system was functioning properly at the given time, the evidence record was tampered, altered or manipulated

[58]https://www.dfrws.org/sites/default/files/session-files/pres-federated_testing_shared_test_materials_from_the_cftt _program_at_nist.pdf .
[59] Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework, 27 February 2012, pp.14.
[60] LUND, STEVEN/IYER, HARI, Likelihood Ratio as Weight of Forensic Evidence: A Closer Look, Vol. 122, Art. 27, Journal of Research NIST, 2017.
[61]CATHY O'NEIL, Weapons of math destruction: how big data increases inequality and threatens democracy, New York: Crown Publishers, 2016; https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/ CALO, RAYN, Artificial Intelligence policy: A roadmap – draft; https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing;
[62] ENFSI action plan 2016-2017: http://enfsi.eu/wp-content/uploads/2017/02/7.0-ENFSI-Action-Plan-2016-2017.pdf
[63] ROYAL STATISTICAL SOCIETY, THE INNS OF COURT COLLEGE OF ADVOCACY, Statistics and probability for advocates: Understanding the use of statistical evidence in courts and tribunals, 2017.
[64] IBID., MASON, 6.194.

by third person, which can include also contamination by the forensic examiner. Cross-verification and reproducibility of forensic results is also particularly important for the defence.

One approach is the access to the software source code, in order judges and forensic specialist to evaluate possible errors or modifications. Therefore, *Mason* calls for disclosure and discovery of source code under confidentiality agreements[65], but finds negative unwillingness of judges and lawyers to request cross-testing of system audits and critical updates[66]. A federal judge recently unsealed the source code for a software program developed by New York City's crime lab, exposing to public scrutiny a disputed technique for analysing complex DNA evidence[67]. In this respect standards for open source software increase the verifiability.

While both *Mason* and *Casey* agree on the danger of applying presumption of reliability to computer systems, considering the numerous existing hardware and software errors, *Casey* argues that "it is more effective to focus on the evidence itself rather than the reliability of the process that created it" as well as searching for "further corroborating information" from other sources[68]. He also discusses the importance of peer review of the forensic results by other DF specialist and with different methodologies and refers to *Sommer* on prehearing of experts, when there are disagreements on the results. However, the challenges outlined by both authors, as legal and digital forensics ones are related to what constitutes an adequate test for different types of digital data, which are the right mechanisms to determine error rates, how to incorporate probative value, quality, integrity and reliability in the evidence itself and how adequate interpretation and challenging of forensic findings are[69]. According to these results, global standardization of evidence is narrowly understood as setting this type of data under specific regime in order to improve the quality of its assessment, which consequently may open the dialog for some harmonization of legal systems and comparative reasoning by lawyers and judges.

5. Data protection and forensics

Walden reminds that "although European data protection laws apply only to personal data, their practical impact may be broader […] because it may be difficult to delineate personal data (for example where they are co-mingled with non-personal data or where they are encrypted)." Here, we examine two issues in the data protection regime, which are considered the most challenging for compliance in digital forensics, but with a very significant impact on the admissibility of digital evidence: namely, the vague regulation of external digital forensic services in data protection law and the gaps by estimating the intrusiveness of the investigation measure. In both cases, a standardization approach may provide practical solutions.

Svantesson argues that in an investigation context the "recognised, distinction between (a) subscriber data, (b) traffic data and (c) content data, does not match data privacy law's distinction between (a) non-personal data, (b) personal data and (c) sensitive personal data"[70]. The Commission recently replied, "Subscriber information, traffic data, metadata, and content data are personal data, and are thus covered by the safeguards under the EU data protection acquis"[71]. Nonetheless, the CoE cloud evidence group reports that in the majority of criminal cases (60%) only traffic and subscriber information need to be collected, which is a lesser interference with data subject rights[72].

---

[65] IBID,.
[66] IBID., 6.196, 6.222, 6.225, 6.229.
[67] https://www.propublica.org/article/federal-judge-unseals-new-york-crime-labs-software-for-analyzing-dna-evidence?lipi=urn%3Ali%3Apage%3Ad_flagship3_profile_view_base_recent_activity_details_all%3BWC4JYmrUQJWXLT%2FzNHXOYA%3D%3D .
[68] IBID., pp.62 and pp.69.
[69] IBID., CASEY, pp.74; MASON 6.84.
[70] SVANTESSON, DAN, Preliminary Report: Law Enforcement Cross-Border Access to Data, 2016.
[71] IBID., Note 9554/17, pp. 46.
[72] https://rm.coe.int/16806bdafd .

The Directive 2016/680/EU[73] has a wider scope and includes any processing of personal data, nationally or internationally. It introduces sector specific rules – distinguishes different data subject categories[74] and requires separation of hard (based on facts) and soft (based on assumption) data and independent oversight as well (Art. 6 and Art.7). In addition, the separation of certain categories of personal data under different protection regimes is established in Convention 108 and in R (87) 15 as well[75]. In compliance with Convention 108 most police and law enforcement authorities have already developed data protection regimes; so – depending on the congruence with legacy systems – it may be challenging to harmonize and adapt the existing police systems to the new requirements. Moreover, external digital forensic services, which only assist with forensic analysis to the investigation, must also apply such data protection rules. Sadly, it is not clear in the Directive which rules apply for cases in which personal data is being transferred to private parties for law enforcement purposes in and outside EU, or when police authorities are using data for a law enforcement purpose, but incompatible with the one for its prior collection (Rec. (11) and Art. 9). However, both are of importance in terms of cross-border exchange of evidence. For both LEAs and digital forensic services, it is important to understand under which conditions data must be communicated to data subjects with respect to data subject's rights, fair trial and defendant`s rights.

The intrusiveness of a certain law enforcement measure is evaluated by data protection principles (Art. 8 (2) ECHR and ECrtHR standard test[76]), namely it must be first provided for by law, second serve a legitimate aim and thirdly be necessary and proportionate in a democratic society. CJEU in the *Schwartz case* provides also a method to apply the necessity and proportionality test[77]. In addition, the *WP29* has published practical recommendations, where the evaluation depends on the social need, the safeguards applied, preventing excessiveness, limits of the retention, but also on abstract concepts like purpose limitation, margin of appreciation and culture in MS[78]. In the latest communication the Commission points out, that the necessity and proportionality test depend on the type and volume of evidence, the type of investigation measure, its intrusiveness and safeguards to human rights[79]. It is not realistic, though, to assume that forensic experts can limit their collection methods only to relevant data from the beginning, or that all experts, which are often not lawyers, can successfully conduct a complex legal test. Simultaneously, cases where judges will need to refuse to accept important evidence due to the warrant's limits being exceeded, will need to be avoided. A clearer standard needs to be developed to overcome this legal gap. As argued by *Hong and Yu* a "model needs to be established that can assess and regulate excessive search and seizure of digital evidence in accordance with a reasonable standard that considers practical limitations."[80] Practical application of the purpose limitation principle is very challenging, considering that forensic experts may follow only traces online until they find concrete evidence; and not always it is possible to *ex ante* define precisely the needed information type or content, or the forensic method appropriate. In addition, the principle is set under pressure by the examined above EU data bases (SIS II, VIS,

[73]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.

[74]Four categories of data subjects (suspects, criminals, victims and third parties) according to its relation to the crime proceedings and must be treated under different regimes by the police authorities.

[75]Convention 108 – Art. 6 and Art. 12 (3) (a); R (87) 15 in Principles 3 and 7.

[76]KORFF, DOUWE, The standard approach under Article 8 – 11 ECHR and Article 2 ECHR.

[77]Schwarz v. Stadt Bochum, ECJ, C-291/12, Judgment of the Court of 17 October 2013, para 34.

[78]ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, adopted on 27 February 2014.

[79] IBID., 9554/17 tech doc, part V.C., pp.46.

[80] ILYOUNG HONG/HYEON YU/ SANGJIN LEE/ KYUNGHO LEE, A new triage model conforming to the needs of selective search and seizure of electronic evidence. Digital Investigation, 10(2), 175-192, 2013.

EURODAC, ESS)[81], which are created for other purpose but will be used also for law enforcement activities, which is direct violation of purpose limitation.

The need of data retention for investigation purposes is well recognized by law enforcement authorities, but fundamentally questioned and criticised within the data protection community; and data retention also affects the cooperation with private sector. The controversial nature of the data retention laws is partially rooted in the apparent inability of the legislator to guarantee sufficient safeguards, and maintain an appropriate necessity and proportionality test for data retention, which was also received emphasis by CJEU when invalidating the Data Retention Directive[82]. However, the UN report concluded that "National legal obligations and private sector data retention and disclosure polices vary widely by country, industry and type of data. Some countries report challenges in obtaining data from service providers"[83].

6. Conclusions

The paper examines the emergence of legal, scientific and technical standards in the digital evidence domain and its impact as quality assurance in law-making, court proceedings and digital forensics. New regulation on evidence exchange in Europe, improving MLA regimes and EIO implementation will greatly depend on the ongoing standardization initiatives for better facilitation and security in the evidence chain of custody and their national implementation. As main standardization topics are outlined legal evaluation and challenging forensic findings in court, adequate tests for different types of digital data, mechanisms to determine error rates, embedding evidence probative value in forensic process, integrity, reliability and storage of digital evidence, as well as data protection and onsite forensics combined with beck office analytic tools and platforms. Global standardization of evidence is narrowly understood as setting this type of data under specific regime in order to improve the quality of its assessment, which consequently may open the dialog for harmonization of legal systems and comparative reasoning by lawyers and judges. Moreover, both legal and forensic systems require some basic agreements on terminology and taxonomy, interoperable formats, tools and procedures, which also has to facilitate the communication of evidential material with ISPs. In addition, this process will be indirectly influenced by the standards chosen in EU for facilitating exchange through e-Codex and the EU databases.

[81]See fn30. Eu-Lisa must develop anonymization schema for purpose limitation compliance, but the efficiency of the quality measures is yet to be evaluated.
[82]Digital Rights Ireland and Seitlinger and Others ,Judgment of the Court from 8 April 2014 in Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.
[83] IBID., UN report on cybercrime, Key findings on pp. 144.