The Presumption of Innocence as a Source for Universal Rules on Digital Evidence

Stoykova, Radina

Published in:
Computer Law Review International

DOI:
10.9785/cri-2021-220303

lar general defense in the German Copyright law. This decision shows in a very impressive way that such proposals could only work, if in addition to a general exception clause comparable to the fair use clause, certain detailed exceptions were listed in order to provide the necessary level of certainty and predictability, combined with the adequate flexibility to react to new developments which require an adjustment of the Copyright Law.[84]

Dr. Mathias Lejeune

Attorney at Law, Munich, international IT/IP Law, Data Protection and Privacy Law

84 See the respective proposal by *Leistner* IIC 2011, 417.

Radina Stoykova

The Presumption of Innocence as a Source for Universal Rules on Digital Evidence

The guiding principle for digital forensics in producing digital evidence for criminal investigations

This paper proposes a conceptual framework for the development of digital evidence rules in technology-assisted investigations based on the presumption of innocence. The presumption of innocence (PI) is examined as a general principle of criminal procedure to delineate its scope and application on pre-trial and clarify its role for the development and harmonization of practical and enforceable rules for digital evidence. It is demonstrated that the PI provides a theoretical background for digital evidence regulation, digital forensics standards, and harmonized rules on the use of technology for investigative purposes irrespective of jurisdictional differences. The derived PI-based evidence rules reveal missing techno-legal policy for their implementation in digital evidence systems and processes.

After introducing the wide-spread use of digital evidence by law enforcement in the course of criminal investigations and proceedings (I.), this article reviews the schools of thought regarding the impact of PI on evidence procedures focussing on the question whether the PI's protection against wrongful conviction could support measures against arbitrary and intrusive investigations (II.). The reviewing analysis strives to balance contradictory opinions about the scope and application of the PI, before examining digital forensics specifics in the context of the derived PI-based evidence rules to identify techno-legal policy tailored for the digital investigations and its effective implementation in digital evidence systems (III.).

I. Introduction

1 Digital forensic science and evidence have become increasingly relevant in criminal investigations.[1] The investigation stage of the criminal proceedings becomes more pro-active[2] and science-driven[3] in order to deal with growing data complexity and volumes.[4] Due to concerns about efficiency and limited resources,[5] the fact-finding process is shortened, minor cases are more often dismissed while prosecutors frequently use settlements and as a result the pre-trial phase has become more "outcome-determinative".[6] This disruptive change in criminal

1 A report by NCPP in UK points out that 90 % of the criminal investigations have digital element. In Transforming Forensics The UK National Police Chiefs Council, 'Digital Forensic Science Strategy' https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf.

2 Sungmi Park and others, 'A Comparative Study on Data Protection Legislations and Government Standards to Implement Digital Forensic Readiness as Mandatory Requirement' (2018) 24 Digital Investigation S93.

3 E. Murphy, 'The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence', Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 896128, Apr. 2006. Accessed: Feb. 04, 2021. [Online]. Available: https://papers.ssrn.com/abstract= 896128; S. Mason and D. Seng, Electronic Evidence, Fourth. University of London, Institute of Advanced Legal Studies, 2017, para 2.15.

4 FBI statistics show that the size of the average digital forensic case is growing at 35 % per year in the United States, while in 2012 the Computer Analysis Response Team (CART) of FBI supported nearly 10,400 investigations and conducted more than 13,300 digital forensic examinations that involved more than 10,500 terabytes of data. Shams Zawoad and Ragib Hasan, 'Digital Forensics in the Age of Big Data: Challenges, Approaches, and Opportunities', *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems* (IEEE 2015) https://ieeexplore.ieee.org/document/7336350 accessed 16 February 2021. See also Luca Caviglione, Steffen Wendzel and Wojciech Mazurczyk, 'The Future of Digital Forensics: Challenges and the Road Ahead' (2017) 15 IEEE Security Privacy 12; Ibtesam Alawadhi and others, 'Factors Influencing Digital Forensic Investigations: Empirical Evaluation of 12 Years of Dubai Police Cases' [2015] Journal of Digital Forensics, Security and Law http://commons.erau.edu/jdfsl/vol10/iss4/1 accessed 25 February 2021.

5 Mark Scanlon, 'Battling the Digital Forensic Backlog through Data Deduplication' (2016).

6 Shawn Marie Boyne, 'Procedural Economy in Pre-Trial Procedure: Developments in Germany and the United States' [2016] Comparative Criminal Procedure https://www.elgaronline.com/view/edcoll/978178100

investigations, may have led to expect a comprehensive, modernized legal framework around digital evidence to reflect the technological change and provide for fair trial protection, and foremost the presumption of innocence (PI).

2 By contrast, evidence rules are still strongly bound to a specific jurisdiction. An argument for this can be that evidence rules are context-dependent, and their function can be understood only within the norms and values of the specific criminal legal system with its historical and cultural particularities.[7] Moreover, in all traditional criminal jurisdictions evidence regulation is predominantly trial-centric,[8] which strongly contradicts with the ubiquitous and multipurpose use of digital evidence by law enforcement before any charges are officially raised. Even the broad and ambiguous definition of digital evidence refers to "any information of potential probative value that is manipulated, generated through, stored on or communicated by any electronic device".[9] This article refers to digital evidence as the result of digital forensics defined as "the use of scientifically derived and proven methods towards the collection, validation, analysis, documentation and presentation of digital evidence".[10]

3 Consequently, criminal justice principles must guide a larger in scope and scientifically complex digital evidence procedures and technologies with their cross-jurisdictional and cross-disciplinary effects which drastically exceed the deliberate, personalized, and specialised purpose of trial proceedings.[11] Moreover, one cannot negate the underlying criminal procedure principles, forensic science standards, and investigative technology, which does not depend on the jurisdiction and at least in theory must provide a bases for development and approximation of digital evidence rules. For these reasons a set of minimum universal digital evidence rules must be developed. By contrast, standardization bodies[12] are focused on technical guidance for digital forensics not adapted to the law enforcement needs in criminal investigations, while current legislative initiatives on local[13] and international level[14] does not address the digital forensics and digital evidence problematic.

4 This paper examines the potential of the PI as a principle of criminal procedure to provide a theoretical basis for digital evidence regulation, international digital forensics standards, and harmonized rules on the use of technology for investigative purposes which minimize the risks for the judicial process,and specifically for suspects and defendants. The relation between the presumption of innocence and evidence regulation is not apparent. Disquieting conceptual and application differences arise from the principle itself. PI manifestation through evidence rules is well-established on trial and underdeveloped on pre-trial. This introduces dissonance between trial and pre-trial which is intensified by the ubiquity of technology in digital investigations. The analysis here attempts to show that evidence is not merely a sum of procedural mechanisms in different legal traditions, but it has an underlying connection to the presumption of innocence which can be explored and are suitable for approximation of digital evidence procedures in new transnational contexts. The focus therefore is not only on PI-based safeguards but also on digital investigation specifics and the need for practical *implementation* of those rules.

II. PI as Criminal Procedure Principle and its Relation to Evidence Regulation

This Section examines the PI as a fundamental criminal procedure principle and traces its specific application during investigation in order to derive PI-based guiding principles for evidence rules development. The PI is a principle of the criminal procedure which protects suspects, accused, and defendants. The presumption of innocence is internationally recognized in human rights charters and by all international criminal courts and tribunals.[15] It is acknowledged as a non-derogable principle even in armed conflicts and emergency situations.[16] However, there are terminological differences in the codification of the PI, which lead to a disagreement about its meaning and scope on pre-trial. 5

7181/9781781007181.00016.xml accessed 18 February 2020.; Keith Findley, 'Innocents at Risk: Adversary Imbalance, Forensic Science, and the Search for Truth' (2011) 38 Seton Hall Law Review https://scholarship.shu.edu/shlr/vol38/iss3/7.

7 Mirjan Damaska, 'Structures of Authority and Comparative Criminal Procedure' [1975] Faculty Scholarship Series https://digitalcommons.law.yale.edu/fss_papers/1590; John D Jackson, 'The Effect of Human Rights on Criminal Evidentiary Processes: Towards Convergence, Divergence or Realignment?' (2005) 68 The Modern Law Review 737.

8 The civil law jurisdictions emphasise on less evidence requirements on pre-trial and stricter rules on trial (truth-seeking judge, expert opinion rules, reasoned judgements), while the common law traditions rely mostly on trial evidence thresholds and exclusionary rules. See for example Tom Decaigny, 'Inquisitorial and Adversarial Expert Examinations in the Case Law of the European Court of Human Rights' (2014) 5 New Journal of European Criminal Law 149.

9 Mifsud Bonnici, J. P., Tudorica, M. & Cannataci, J. A., 'The European Legal Framework on Electronic Evidence: Complex and in Need of Reform' in Maria Angela Biasiotti and others (eds), Handling and Exchanging Electronic Evidence Across Europe (1st ed. 2018, Springer International Publishing: Imprint: Springer 2018).

10 Gary Palmer, 'A Road Map for Digital Forensic Research, Technical Report (DTR-T001-01)' https://www.dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf.

11 Amber Marks, Ben Bowling and Colman Keenan, 'Automatic Justice? Technology, Crime and Social Control' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2676154 https://papers.ssrn.com/abstract=2676154 accessed 4 February 2021.

12 IEC ISO, 'ISO/IEC 27037 EForensics Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence' (2012) https://www.iso27001security.com/html/27037.html accessed 3 September 2020; ISO/IEC, 'ISO/IEC 27042:2015 Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence' (ISO/IEC 27042:2015, 2015) https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en accessed 4 April 2018; European Network of Forensic Science Institutes (ENFSI), 'Best Practice Manual for Forensic Examination of Digital Technology' https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf.

13 Mifsud Bonnici, J. P., Tudorica, M. & Cannataci, J. A. (n 9).

14 For example, neither the Russian proposal for a UN Convention on Cybercrime nor the Draft Second Additional Protocol to the CoE Budapest Convention which has just finished the consultation stage, seem to include any specific digital evidence and digital forensics standards. For detailed analysis see: Lazaro, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; Malaga, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

15 Art. 21(3) ICTY, Art. 20(3) ICTR and Art. 66 ICC Statute, Art. 48(1) EU Charter of Fundamental Rights; Art. 11(1) Universal Declaration on Human Rights.

16 Human Rights Committee, General Comment, States of Emergency (art. 4); UN Doc CCPR/C/21/Rev.1/Add.11 (2001), §16.

6 Often scholars and regulatory bodies interpret it narrowly as a trial guarantee with limited application during the investigation.[17] Some legal texts define it in relation to criminal proceedings.[18] Others state that the PI applies for the period of any proceedings with a punitive element,[19] while the broadest formulations extend the PI every person irrespective of charge.[20] Lastly, more detailed texts exist, where the presumption is extended to suspects, prosecuted, and accused and relates not only to a broader personal scope but also to evidence requirements.[21] The narrow interpretation of the presumption as a pure procedural guarantee in criminal trials, is contrasted with its broader scope as a fundamental principle of the rule of law.[22] The too broad formulation of the principle as in the civic trust theory or as a substantive right hides a risk to its normative value, its distinction from other rights and safeguards, and could result in lack of enforceability. The too narrow view of the PI as a trial-based principle, however, goes against its fundamentality and could prevent the "translation"[23] of the core protection mechanism of the PI in new social contexts.

1. Civic Trust Theory

7 In a very broad sense, it is argued that the PI is a principle supporting political morality "preserving and concretising trust and respect between the state and its citizens".[24] The theory of "civic trust"[25] suggests that the PI is relevant to the state and all fellow citizens in contexts well beyond the criminal trial while the PI protects individuals also from the burden of becoming a defendant or face a trial. However, arguments that some level of trust in/by all citizens is expression of the PI produces rather moral or ethical implications but has little normative or practical force. As *Weigend* rightfully points out "only the existence of some form of *an 'official' suspicion* (giving rise to the initiation of a criminal investigation) is indeed a necessary condition for the presumption of innocence to spring into action".[26] In fact, civic trust is only realized as normative value in criminal proceedings. The *civic trust theory rightfully extends the PI material and personal scope outside the trial*,[27] but it is imprecise in establishing limits, practical guarantees and enforceability, which are available if the scope is limited to the criminal process as a whole.[28] The civility analysis is insightful for exposing the PI as a *highly context dependent principle, requires practical considerations* such as placing victims and offenders as active participants in the criminal process with rights, but also duties and responsibilities. As too broad, the civility theory is neither enforceable nor normatively supported, the analysis should choose a narrower scope, which however does not limit the principle's strength in any way. This requires examination of the substantive right theory and the theory that the PI is only a trial guarantee.

2. The PI as a Substantive Right

8 Common law scholars have a long tradition of interpreting the presumption of innocence broadly as a substantive human right. *Jackson and Summers* elaborate the substantive right theory in two broader applications aspects:[29]

- individual protection against any intrusive action by the state, understood as justification of any coercive measure undertaken by the authorities; and
- substantive innocence evaluation by courts in cases of wrong criminalization.

Ho even extends the PI as a right to due process, which has an even broader scope than the right to a fair trial.[30] If one considered a substantive right to be treated as innocent, this risks to over-widen the PI's scope to assimilating the legality, proportionality, and fairness principles in criminal procedure. In addition, the right of the individual to require stringent justifications from the state to every coercive measure may "hinder the ability of the police to enforce defensible criminal prohibitions."[31] 9

The difference between other substantive rights and the PI is visible. For example, the ECtHR has stated the impossibility to derogate one's own substantive human rights,[32] but the PI is different as a procedure enforcement tool – many are eager to waive their PI protection in plea bargaining or guilty pleas.[33] However, even in plea bargains and guilty pleas the PI remains a mechanism for procedural protection against wrongful convictions that requires the prosecution to adduce sufficient evidence and cannot rely solely on confession. This places the PI as a procedural protection mechanism in all stages of the crim- 10

17 Committee of Ministers, Guidelines on Human Rights and the Fight against Terrorism, adopted on 11 July 2002 at the 804th Meeting of the Ministers' Deputies, 11 Guideline XV. – Presumption of innocence is first mentioned in IX. (2) Legal proceedings.

18 UDHR, ICPR, Canada, New Zeeland.

19 ECHR, EU CHR Art.48, Constitutions Iran, Italy, Russia, Bulgaria.

20 Rome Statute ICC Art.66, Colombian constitution, Title II, Chapter 1, Article 29; Art.23 Constitution of Romania.

21 See summary about Portugal, France, and South African constitutions: https://en.wikipedia.org/wiki/Presumption_of_innocence#cite_note-32. I/A Court H.R., Case of Zegarra Marín v. Peru. Preliminary Objections, Merits, Reparations and Costs. Judgment of February 15, 2017.

22 Colin Tapper and Rupert Cross, *Cross and Tapper on Evidence* (12th ed, Oxford University Press 2010) 144; Andrew C Stumer, *Presumption of Innocence: Evidential and Human Rights Perspectives* (Hart 2010).

23 See Lawrence Lessig, *Code 2.0* (Basic Books 2010) http://codev2.cc. In Chapter 9, Lessing explains the crucial role of law practitioners to translate the legal principle into the new technological context, as opposed to leaving it hanging on political decisions.

24 Liz Campbell, 'Criminal Labels, the European Convention on Human Rights and the Presumption of Innocence' (2013) 76 The Modern Law Review 681.

25 Nance, DA. Civility and the burden of proof. Harvard Journal of Law and Public Policy, 17, 1994 and Duff, A. Who must presume whom to be innocent of what? Netherlands Journal of Legal Philosophy, 42(3).

26 Thomas Weigend, 'There Is Only One Presumption of Innocence' (2013) 42 Netherlands Journal of Legal Philosophy 193.

27 Campbell (n 24). Dale A. Nance, 'Civility and the Burden of Proof' (1994) 17 Harvard Journal of Law & Public Policy https://scholarlycommons.law.case.edu/faculty_publications/730. Antony Duff, 'Who Must Presume Whom to Be Innocent of What?' (2013) 42 Netherlands Journal of Legal Philosophy 170.

28 Richard L Lippke, *Taming the Presumption of Innocence* (Oxford University Press 2016) ch 6; PJ Schwikkard, 'The Presumption of Innocence: What Is It' (1998) 11 South African Journal of Criminal Justice 396. Weigend, 'There Is Only One Presumption of Innocence' (n 27).

29 John D Jackson and Sarah J Summers, *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions* (Cambridge University Press 2012) 205–211; Andrew Ashworth, 'Four Threats to the Presumption of Innocence' (2006) 10 The International Journal of Evidence & Proof 241.

30 Hock Lai Ho, 'The Presumption of Innocence as a Human Right' in Paul Roberts and Jill B Hunter (eds), *Criminal evidence and human rights: reimagining common law procedural traditions* (Hart Pub 2012).

31 Lippke (n 29) ch 2.

32 See the prohibition of degrading treatment and homeless people wanting to spend the night in jail.

33 Lippke (n 29).

inal process irrespective of which substantive rights the accused chooses to exercise.

3. The PI as a Trial-Based Principle in Various Degrees

11 If one understood the principle as a procedural guarantee, some argue that extending its scope to the beginning of the investigation might limit its normative power, and raise significant controversy about the scope, purpose, and consequences of the PI.[34] According to the proponents of this argument, suspicion-based measures, pre-trial detention, bail proceedings or ex-convict treatment ensure the proper administration of justice and have a broader scope, which is not covered by the PI. However, this is without prejudice to the need for clear evidence procedures, as not all but part of these broad practices results in criminal investigations, and moreover they have a significant impact on the burden of proof (BoP). The process of proving "legal guilt or innocence" as opposed to factual reasoning, absorbs "procedures of sustaining the charge" and in essence, relates to evidence procedures, which mitigate the dangers to the BoP and the rights of the innocent defendant.

12 *Therefore, the PI has a function in the whole criminal process to include safeguards to the BoP. As Risinger* argues "[i]t is in the pretrial stage that the weaknesses of our inherited adversary system are most extreme and most apparent, and most in need of change to benefit the innocent".[35] Further, this view is supported by *Findley*, who examines "skewing mechanisms" in the early stages of the investigation, which allocate the risk of error and uncertainty to the suspect.[36]

13 Indeed, the investigation to a great extent is concerned with procedures to prove guilt, but it is also a part of the criminal process as a whole,[37] and must be guided by the same principles as the trial stage. On the other hand, seen only as a component of the criminal process, the trial can only be fair if such procedures for establishing guilt are just and in compliance with the PI.

14 However, there are significant differences between the investigation and the trial in their purpose and objectives, which will require a different approach to implementation of the fairness safeguards. The trial purpose is to verify if guilt beyond reasonable doubt based on the evidence is proved; while the pre-trial dominates and leads the evidence procedures which can meet this standard; in both, however, quality of evidence and protection for the innocent is required. During the investigation the level of uncertainty about past events, the risks of error, the risks to the BoP, and the risks to accuracy – all fundamental parts of the administration of justice, are much higher than at trial. Prevention procedures could be employed where higher risks of error and uncertainty are accepted by the legislator, in order to allow the police to react promptly to immediate danger. Moreover, the equality of arms principle could be fully realized only at trial, while pre-trial rules only support the notion. Sometimes during the investigation conflicts may arise as to how much fair trial guarantees could be respected without jeopardizing the reliability of the evidence or what are the highest procedural safeguards available without jeopardizing the effectiveness of the prosecution. Therefore, it could be concluded that *mere transposition of trial guarantees to the investigation stage will be unsatisfactory and potentially ineffective*. Both the trial and the investigation are guided by the same procedural principles, but the investigation, given the observed specifics, *requires a different implementation approach to achieve the same legislative goals*.

15 It is not a viable argument either that the PI is particularly stringent on trial, but weak on pre-trial or that if the PI mechanisms are too strong on pre-trial, they will hamper the effectiveness of the investigation. The PI doesn't change its strength throughout the criminal process, though the pre-trial has a different purpose. The PI protects BoP and process integrity by requiring any errors or uncertainties to be documented and mitigated during the whole criminal process. Note, that the PI does not require all procedures at the investigation stage to meet the standard of proof. *The lack of information of what on pre-trial is considered reliable evidence, how it was obtained, or how was tested, is what is contrary to the PI, because it prevents further evaluation of the facts and sets a disproportionate risk for the innocent defendant. Therefore, the PI requires an accountable investigation process. In this respect, the difference between the trial and the investigation is not in the strengthof the PI principle, but in the implementation and enforcement approach.*

16 As examined with respect to the civic trust theory, the idea for different degrees of the PI protection, differences in its strength of application, or the argument that the PI is "partially rebutted"[38] in the early stages of the investigation when coercive measures are authorised, contradicts the fundamentality of the principle.

4. Evidence Thresholds: The PI vs. BoP

17 Many authors in the Anglo-American legal tradition defend the idea that the PI requires a certain threshold of suspicion and evidence before the exercise of any powers on the individual.[39] The claim that a certain threshold of evidence is required to rebut the PI is at first glance unsettling in the civil law systems, where the parties are not active and in non-adversary settings the prosecution does not have a burden to prove *per se*. Moreover, the burden and standard of proof have a broader scope than the PI at trial related to many additional

34 Schwikkard (n 29); Elies Van Sliedregt, 'A contemporary reflection on the presumption of innocence' (2009) Vol. 80 Revue internationale de droit penal 247.

35 D Michael Risinger and Lesley C Risinger, 'Innocence Is Different: Taking Innocence into Account in Reforming Criminal Procedure' 56 41.

36 Findley (n 6).

37 Ashworth, A. (2003). Exploring the Integrity Principle in Evidence and Procedure. In P. Mirfield and R. Smith (Eds.), Essays for Colin Tapper. London: LexisNexis. He describes the relation between the trial and the investigation as follows: 'The trial is not simply a sealed component, [...] if one reflects on the purpose of many of the pre-trial activities of state officials ... The purpose is largely to obtain evidence, or "leads" that may produce evidence, with a view to constructing a case against the suspect. ... [T]he very motivation for almost all pre-trial activities is to prepare the ground for the trial.'

38 Ibid., Lippke refers to Ho.

39 Kim A. Taipale, 'The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence' (2005) 20 IEEE Intelligent Systems 80; Marianne Hirsch Ballin, 'Inside View of Dutch Counterterrorism Strategy: Countering Terrorism through Criminal Law and the Presumption Innocence Panel Session Papers/Articles': (2008) 8 Journal of the Institute of Justice and International Studies 139.

facts outside the guilt-innocence alternative (e.g., mitigating or aggravating circumstances, procedural facts, etc.)[40] and therefore according to scholars not the PI but the BoP guides evidence rules.[41]

18 On pre-trial, however, the BoP is expressed only by processes and technical evidence rules for accuracy. The PI aim is different: to protect the suspects and defendants from the negative effects of the investigation, which may in some cases increase accuracy, but may as well, set limits to the striving for evidence and conviction. In this respect, an investigation measure which requires suspects to give proof about their innocence will hamper the integrity of the criminal process even if it produces accurate evidence. Requirements like the strict proportionality assessment of investigation measures, limiting the use of power based on assumptions of guilt, mitigating errors in the investigation, degree of suspicion before exercising coercive measures, are in practice additional evidence rules and thresholds based on the PI, which have little to do with the technical evidence rules based on the BoP during trial. Indeed, the burden and standard of proof determine the evidence threshold necessary to find a defendant guilty, but the PI determines the evidence thresholds for proving that the innocent suspects and defendants were *protected from the negative risks of the investigation process*. The PI mitigates the risks of false conviction on which the burden and standard of proof are based. *Robert and Zuckerman* consider that there is a "practical demand" for individuals to have an "effective protection from the depredation of criminality and a *reasonable measure of security* to go about their lawful business unmolested".[42] These arguments are more consistent with the evolution of the PI as a human right and account for the sophistication, internationalisation, and expansion of contemporary investigations as "outcome determinative".

5. The PI and Best Evidence Rules

19 As a rebuttable presumption of criminal law, *Roberts and Zuckerman* argue, it is a set of rules, which "permit or require presumed facts to be established by operation of law".[43] The authentic PI role is that it is binding on the fairness standard of all processes and parties involved in the "legal", criminal evidence production, even when the evidence procedure is not directly related to the accused's "factual" guilt or innocence. This function is sometimes discussed as counterfactuality.[44] As a mechanism, which preserves the integrity of the evidence production process, the PI has the role to ensure the practical and effective protection of innocent suspects and defendants as well as the most accurate procedure which will satisfy the BoP on trial.

20 Because in the criminal process the stakes for both the state and the individual are high, the risk of error must be reduced to a minimum. Protecting the innocent defendant from the risk of low-probative evidence can be achieved by requiring standards and quality in the investigation procedure which allocates the risk of error to the prosecution. It could be also achieved on trial trough rules such as best evidence[45] and exclusion,[46] typical of the common law system. Moreover, introducing PI-based evidence rules at the investigation stage benefits quality assurance and reliability testing, which reduce the need for exclusion. Exclusions must be reserved as a last remedy, while risk allocation can depend on the quality standards of procedure.

Stein accounts for the multidisciplinary field in which the PI and evidence rules are operating. He formulates two evidence principles with significant importance for the PI and its application on pretrial. The best evidence principle states that fact finding for legal purposes must use the "most reliable sources of information and follow the most effective procedures for testing information". However, in practice this epistemological principle is not fully applied in criminal procedures due to resource constrains and cost-efficiency considerations. Therefore, he further argues, the principle of maximal individualization (PMI) must be followed. PMI requires that "fact-finders must receive and consider all case-specific evidence [...] and the evidence upon which this argument rests exposed to and survived maximal individualized examination." 21

6. The PI as a Rule of Judgement or Rule of Treatment?

Although the proponents of the PI in the narrow sense refer to it as a rule of treatment, they do not really explain what it means to be "treated" in compliance with the PI, and why it is a requirement also at the investigation stage. *Lipkke* argues that a requirement for a "corrective attitude" towards the accused is illusionary in practice, calling it "unhelpful and, at worst, likely to be cynically dismissed" and concludes that the best one can expect at the pre-trial stage is "*non-presumption of probative guilt*", which will discourage the authorities to "rush to premature or conclusive judgments concerning the material or probative guilt of suspects".[47] This view is typical for the US doctrine which recognizes the PI as a rule of judgement, and not as a rule of treatment[48] 22

Hock Lai Ho, to the contrary, claims that the PI as a human right "is directed against the state; and on the proposed theory, the trial is the political process of holding the executive to account on its quest to get a person officially condemned and 23

40 Mirjan Damaska, 'Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study' (1973) 121 University of Pennsylvania Law Review 506.

41 Schwikkard (n 29); Thomas Weigend, 'Assuming That the Defendant Is Not Guilty: The Presumption of Innocence in the German System of Criminal Justice' (2014) 8 Criminal Law and Philosophy 285.

42 Paul Roberts and AAS Zuckerman, *Criminal Evidence* (2nd ed, Oxford University Press 2010) 189.

43 Ibid 233.

44 Weigend, 'There Is Only One Presumption of Innocence' (n 27); Ferry de Jong and Leonie van Lent, 'The Presumption of Innocence as a Counterfactual Principle' (2016) 12 Utrecht Law Review 32.

45 Dale Nance, 'The Best Evidence Principle' (1988) 73 Iowa Law Review Faculty Publications 463 https://scholarlycommons.law.case.edu/faculty_publications/463.

46 M Redmayne, 'The Structure of Evidence Law' (2006) 26 Oxford Journal of Legal Studies 805; Alex Stein, *Foundations of Evidence Law* (Oxford University Press 2005).

47 Lippke (n 29) ch 6.

48 Shima Baradaran Baughman, 'Restoring the Presumption of Innocence' (Social Science Research Network 2011) SSRN Scholarly Paper ID 1757624 https://papers.ssrn.com/abstract= 1757624 accessed 17 July 2020; Francois Quintard-Morenas, 'The Presumption of Innocence in the French and Anglo-American Legal Traditions' (2010) 58 The American Journal of Comparative Law 107.

punished".[49] The burden and standard of proof require accuracy, but the evaluation of the quality of the procedure to achieve accuracy is guided by the PI principle. Contrary to Ho's political morality theory, the PI requires a standard of procedure to be met in the investigation to the benefit of both the innocent defendant and the prosecution. For example, *clear evidence rules instruct the investigator on how to deal with uncertainties in the evidence process, how to work in order to meet the BoP, and ensure that the decision-making process at the investigation stage will be based on the same principles as on trial.*

24 Indeed, the PI has a practical implementation as evidence rule to enforce certain ways of treatment of suspects or accused but it has little to do with an "illusionary attitude" or a "right against the state". *What the PI requires morally is an open-minded fact-finder, but legally to the contrary, it requires practical mechanisms and safeguards that whatever attitudes, uncertainties or biases are part of the investigation, their impact will be minimized and procedurally mitigated as much as possible.* The development of such procedures for evidence is the practical and enforceable expression of the PI requirement. Moreover, such error mitigations at different investigation stages must be additionally produced in evidence. In addition, the PI can "inform various aspects of professional ethics".[50]

III. The PI Implications to Digital Investigations

25 The literature review shows that the PI is a procedure enforcement mechanism which allocates the risk of error, demands high evidence standards, prevents from abuse of power, protects fair administration of justice, and activates the defendant stand for the evidence examination in the criminal proceedings. Further examination of the digital forensics (DF) specifics in the context of the identified PI-based evidence rules allows to define a techno-legal policy tailored for the digital investigations and its effective implementation in digital evidence systems.

1. Legal Basis of Digital Forensics (DF)

26 The first principle identified in 2.1.–3. above, to be transposed to the digital evidence domain is that the PI has a function from the beginning of the evidence handling to include safeguards in procedures with the bearing on the BoP. In contemporary settings the PI scope cannot be narrowed to the trail. The evidence production in digital investigations has largely shifted to the investigation and includes many stages and actors whose decision-making process cannot be scrutinized on trial and exceeds its objectives. The scientisation of the digital investigation process and reliance on technology means that in addition to scientific standards, the PI must *transpose criminal justice values to digital forensic science and technology*.

27 To ensure quality of law and procedure, regulation of digital investigation measures demands procedural safeguards such as time limits, authorisation based on facts, judicial oversight, etc. However, the legality of the forensics sciences has always been an open question.[51] Traditional forensics (e.g. hair and fibre, ballistics, handwriting) are observational, provide a narrow information for the investigation, while DF have broad application, claim scientific robustness, and require multidisciplinary expertise to be validated.[52] To ensure legal certainty and consistent treatment of suspects with respect to their data, the legal bases of the DF method and tools must be defined, as well as lawful purpose and use of technology. Regulation of lawful use and purpose in combination with reliability standards can guide evidence admissibility for novel DF methods and tools which are not yet regulated by law. This can also assist in proportionality assessment of DF method and tool, limiting the use of technology based on assumptions of guilt, mitigating bias in the investigative methods, and setting probability thresholds for intrusive technology.

2. Active Defence Forensics

28 It is not possible to transpose defence evidence rights from trial to the investigation stage since as observed *in 2.3. above*, the investigation has different objectives and principles like equality of arms, transparency, and defence access to the evidence cannot be fully realized. In most jurisdictions many reasons are examined as to why traditionally defendants are disadvantaged in respect to forensic reports.[53] Contemporary DF procedures deal with huge amounts of data available for investigation but not necessarily for the trial, limited resources, and technical complexities of the methods employed. The DF report does not necessarily reflect how methods and tools are applied for evidence processing.[54] Often the relevance and weight of technical expertise is taken for granted,[55] while challenging it on reasonable grounds requires a level of technical literacy, access to initial datasets, method, and tools validation information. Therefore, technology-assisted investigations can be set in more deliberative and participatory discourse. Placing victims and offenders as active participants in the criminal process can ensure human rights compliance,[56] but also increase rationality and consistency in digital investigation. Having the right to cross-examine the forensic report once it cannot obstruct the investigation, to ask the forensic examiner questions or request search for exculpatory evidence, and to have the right to explanation of the method and tools used – can solve factual issues in a DF procedure prior trial and save trial resources for the legal evaluation of the facts.

49 HL Ho, *A Philosophy of Evidence Law: Justice in the Search for Truth* (Oxford University Press 2008).

50 Gary Edmond and Andrew Roberts, 'Procedural Fairness, the Criminal Trial and Forensic Science and Medicine' (2011) 33 FORENSIC SCIENCE AND MEDICINE 36.

51 JF Nijboer and WJJM Sprangers (eds), *Harmonisation in Forensic Expertise: An Inquiry into the Desirability of and Opportunities for International Standards* (Thela Thesis 2000).

52 Erin Murphy, 'The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence' (Social Science Research Network 2006) SSRN Scholarly Paper ID 896128 https://papers.ssrn.com/abstract= 896128 accessed 4 February 2021.

53 Decaigny (n 8); Joëlle Vuille, Luca Lupària and Franco Taroni, 'Scientific Evidence and the Right to a Fair Trial under Article 6 ECHR' (2017) 16 Law, Probability and Risk 55.

54 Helen Page and others, 'A Review of Quality Procedures in the UK Forensic Sciences: What Can the Field of Digital Forensics Learn?' [2018] Science and Justice https://research.tees.ac.uk/en/publications/a-review-of-quality-procedures-in-the-uk-forensic-sciences-what-c accessed 25 March 2020.

55 Gary Edmond and Andrew Roberts, 'Procedural Fairness, the Criminal Trial and Forensic Science and Medicine' [2011] Sydney Law Review 1.

56 Jackson and Summers (n 30) ch 7.

29 Legal basis and purpose of DF methods and tools in combination with active defence forensics rights forms a legislative approach to DF which can be complemented with multi-disciplinary oversight. However, this legal approach strongly depends on technology and process level accountability and reliability standards, to develop systems that can produce the information necessary for legislative intervention and to implement PI-based evidence compliance mechanisms.

3. Accountability and Integrity of Digital Evidence Process

30 The PI is a procedural protection mechanism that requires integrity and accountability throughout the entire evidence production process, which can be translated to DF as (i) a reliability standard and (ii) obligation for transparent logic of the processing.

31 In order to ensure integrity of the evidence production process, the DF methods must be sufficiently documented. PI demands not only documenting origin, accuracy, and integrity preservation of the data sets but also justification of the digital forensic actions according to the forensic task and investigative objective. PI-based evidence rules to instruct the investigator on how to deal with uncertainties in the evidence process and how to produce auditable records of the digital forensic actions are necessary for achieving higher specification of values and norms in intrusive technologies for law enforcement purposes and exposing flaws in professional practices, which must further be addressed by regulation. Practical mechanisms for accountability in the digital forensic investigations can demonstrate the logic of the evidence processing, and therefore demonstrate compliance with PI.

a) Digital Evidence: Reliability Standards

32 Current digital forensic practices are not sufficiently tested for their reliability and do not provide documentation for validation and audit. The lack of legal reliability standard in combination with data volumes and complexity,[57] lack of resources and formal validation procedures are often used as an argument for not implementing quality standards.[58] Reliability validation crisis in digital forensics was discussed by scholars[59] and governmental bodies worldwide.[60] Several legal scholars called for DF expert accreditation[61] and discussed the absence of clear legal rules for evidence reliability assessment as a disadvantage for suspects and defendants.[62]

33 The lack of reliability testing and accountability in current DF practice introduces a disproportionate risk for innocent suspects and defendants. Before the digital evidence reaches trial (if it reaches trial) – it is unclear how data was processed, whether the DF techniques were suitable and proportionate to the investigative task, and if the tools used by law enforcement were validated. Depending on the skills of DF experts and the technology available suspects and defendants could be treated differently in similar cases which challenges legal certainty. It also poses questions about lawful and fair use of investigative technology, impartiality of the forensic examiners, and access of the defence to forensic aid.

34 Reliability and fair use of technology for investigative purpose is a common ground for international regulation and standardisation. Rapid technology development and dynamics in DF hinder strict exclusion or formal expert requirements in favour of reliability testing standards. Firstly, exclusionary rules are criticized as an inadequate method to scrutinize technical evidence,[63] especially in a domain like DF where scientific and non-scientific expertise is merged. Even if exclusionary rules are introduced in the legal system, the admissibility of DF examiner report must be based on evaluation criteria for its relevance and reliability to the fact at issue. Secondly, scientific complex methods and tools used in digital investigation require reliability testing standards to be implemented on process-level, which might reduce the exclusionary evaluation to a formal compliance. Reliability validation of DF methods also supersedes formal requirements.[64] Even certified experts might introduce errors and bias in the examination of digital data, while reliability testing expose errors on application level with respect to tools, methods, and examiners work. Some DF domains require very specific expertise, which might not be included in DF expert's accreditation.

57 Graeme Horsman, 'Framework for Reliable Experimental Design (FRED): A Research Framework to Ensure the Dependable Interpretation of Digital Data for Digital Forensics' (2018) 73 Computers & Security 294; Andy Jones and Stilianos Vidalis, 'Rethinking Digital Forensics' (2019) 3 Annals of Emerging Technologies in Computing 41.

58 Radina Stoykova and Katrin Franke, 'Standard Representation for Digital Forensic Processing', *2020 13th International Conference on Systematic Approaches to Digital Forensic Engineering (SADFE)* (2020).

59 Nicolas Hughes and Umit Karabiyik, 'Towards Reliable Digital Forensics Investigations through Measurement Science' (2020) n/a WIREs Forensic Science e1367; Graeme Horsman, 'Framework for Reliable Experimental Design (FRED): A Research Framework to Ensure the Dependable Interpretation of Digital Data for Digital Forensics' (2018) 73 Computers & Security 294; Eoghan Casey, 'The Chequered Past and Risky Future of Digital Forensics' (2019) 51 Australian Journal of Forensic Sciences 649; Jones and Vidalis (n 58).

60 'PCAST Releases Report on Forensic Science in Criminal Courts | Whitehouse.Gov' https://obamawhitehouse.archives.gov/blog/2016/09/20/pcast-releases-report-forensic-science-criminal-courts accessed 6 March 2020; Council of the European Union, 'Draft Council Conclusions on the Way Forward in View of the Creation of an European Forensic Science Area' http://data.consilium.europa.eu/doc/document/ST-6078-2016-INIT/en/pdf accessed 27 March 2018.

61 Hans Henseler and Sophie van Loenhout, 'Educating Judges, Prosecutors and Lawyers in the Use of Digital Forensic Experts' (2018) 24 Digital Investigation S76; NJM Kwakman and others, 'Expert Registers in Criminal Cases. Governance in Criminal Proceedings' https://www.rug.nl/rechten/congressen/archief/2011/governancemeetslaw/workingpapers/papernijboerkeulen.pdf accessed 25 June 2020.

62 D Risinger, 'The Five Functions of Forensic Science and the Validation Issues They Raise: A Piece to Incite Discussion on Validation' (2018) 48 Seton Hall Law Review https://scholarship.shu.edu/shlr/vol48/iss3/6; Gary Edmond, 'Is Reliability Sufficient? The Law Commission and Expert Evidence in International and Interdisciplinary Perspective (Part 1)' (2012) 16 The International Journal of Evidence & Proof 30; Peter Sommer, 'Forensic Science Standards in Fast-Changing Environments' (2010) 50 Science & justice: journal of the Forensic Science Society 12; Michael J Saks and Jonathan J Koehler, 'The Coming Paradigm Shift in Forensic Identification Science' (2005) 309 Science (New York, N.Y.) 892.

63 Sabine Gless and Laura Macula, 'Exclusionary Rules-Is It Time for Change?' in Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules* (Springer International Publishing 2019) https://doi.org/10.1007/978-3-030-12520-2_12 accessed 29 October 2020; Thomas Weigend, 'The Potential to Secure a Fair Trial Through Evidence Exclusion: A German Perspective' in Sabine Gless and Thomas Richter (eds), *Do Exclusionary Rules Ensure a Fair Trial?*, vol 74 (Springer International Publishing 2019) http://link.springer.com/10.1007/978-3-030-12520-2_3 accessed 27 January 2020. Ryan Goss, 'Out of Many, One? Strasbourg's Ibrahim Decision on Article 6' (2017) 80 The Modern Law Review 1137.

64 Henseler and van Loenhout (n 62); Kwakman and others (n 62).

b) Documenting the Logic of the Processing

35 Legal reliability standard cannot be developed without a validation process which documents the logic of the processing in each forensic task. Such logic consists of three elements:

36 Technology Documentation: To make the algorithmic processing transparent one must examine the suitability of the selected algorithm for the concrete forensic task and detect any errors in the execution of the algorithm. Technology level documentation must provide information about the employed functionality of the automated setup. This may include information about tool, version, configuration, algorithm and implementation. Important are also references to previous validation and verification testing and stating known errors reports e. g. data interpretation limitations, bugs in the version, and tool's ability to report errors in output.

37 Methodology Documentation: Validation of the method is an "assessment of weather a standardized sequence of steps, often employing digital forensic tools, leads to a reliable result.[65] The DF examiner must provide documentation that she followed accepted scientific approaches and any deviation from such must be justified. The examiner might refer to peer-reviewed method, established practice or previous work. The minimum information necessary for reliability validation must include experiment or test setup, test data set description, pre-processing for input, algorithm and feature selection.

38 Application Documentation: On application level the examiner must ensure that the method and tool work correctly and as intended in the concrete case. Humans could introduce bias and errors in the evidence processing[66] even though the algorithms are operational.[67] Reliability documentation must contain minimum description of subjective measurements e.g. hypothesis, assumptions, statistical and expert knowledge. Examiner's interaction with the tool must be traceable and includes justification of method, algorithms, and features selection according to method specifications. Concluding remarks must express confidence level, precision and accuracy, while there must be a clear separation of facts from inferences. Automated documentation and verification can decrease the need of exclusionary rules and ensure cost-efficiency at scale.

4. PI by Design and Error-Mitigation Mechanisms

39 PI as a rule of treatment requires protection from the negative risks of the investigation process and PI-based error mitigation mechanisms to be implemented in evidence management systems. *Hildebrandt* proposed that the notion of *PI by design* should be operationalized in data-driven criminal investigations.[68] In addition to reliability standards and documenting the logic of the processing, developed in *Section 3.3.2*, the last technological aspect examines PI-based principles for machine and human error mitigation mechanisms in the design of investigative technology.

5. Procedural Rationale for DF Error Mitigation

40 According to Stein the burden and standard of proof set the probability thresholds, while exclusionary, pre-emptive, corroboration and cost-efficiency evidence rules are dealing with the risk of error and consequently of wrongful conviction.[69] Stein's argument is that a trial-centred, economic utilitarian theory is preferable in the evidence domain than the procedural rights theory adopted here because evidence rules are instrumental and achieving certain social goal with respect to the state's limited resources. This view is very important because it explains the relation between the need to allocate limited resources for DF investigations, the harm which inaccuracy can cause and the moral and political choice to accept or not certain risks. However, such cost-efficiency evaluation could not take place on global scale, as digital evidence requires, if one does not agree on minimal procedural guarantees in the first place. In other words, *the instrumentality of evidence rules can facilitate, but not replace their procedural rights rationale*. Instrumental evidence rules cannot solve important fact-finding questions related to infringements of the PI for the benefit of efficiency and circumventing other human rights e.g. privacy and security on the benefit of accurate fact-finding. The answers of those questions must come as decision by elected representatives. By introducing new technology in investigations, one delegates these moral and political choices, not to judges, but to those operating the technology itself. Operationally, examination of *costs of errors vs. the cost of error-avoidance mechanism*, requires an evidence case management system, which is transparent on process level and can track back the investigative actions of both machines and humans. Technology allows automated documentation and verification which can decrease the need of exclusionary rules on the benefit of universal procedures for reliability validation.

a) Best Evidence Rule

41 The concept of "*original*" in digital evidence context should be understood as the forensic copy of a raw data set, because only controlled digital forensics procedure allows to evaluate the integrity and reliability of the data adduced as evidence.

42 In DF the best evidence rule requires the examiner to use the most accurate procedure for fact-finding "in preference to a form of evidence based on a technique or theory the reliability of which has not been or cannot be tested".[70] Although not explicitly defined, the best evidence rule in the digital domain depends on data availability and volatility.[71] To implement this rule a system must support documentation outline in paras. 35–38 above.

65 Hughes and Karabiyik (n 60).

66 Nina Sunde and Itiel E Dror, 'Cognitive and Human Factors in Digital Forensics: Problems, Challenges, and the Way Forward' (2019) 29 Digital Investigation 101.

67 Engin Bozdag, 'Bias in Algorithmic Filtering and Personalization' (2013) 15 Ethics and Information Technology 209.

68 Mireille Hildebrandt, 'Criminal Law and Technology in a Data-Driven Society' in Markus D Dubber and Tatjana Hörnle (eds), *The Oxford Handbook of Criminal Law* (Oxford University Press 2014) http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199673599.001.0001/oxfordhb-9780199673599-e-9 accessed 12 August 2020.

69 Stein (n 47).

70 Edmond and Roberts (n 51).

71 RM Morgan, 'Conceptualising Forensic Science and Forensic Reconstruction. Part II: The Critical Interaction between Research, Policy/Law and Practice' (2017) 57 Science & Justice 460.

b) Corroboration Rule

43 Pieces of digital evidence are usually scattered across systems and network[72] and corroboration rules are crucial to examine if the evidence reconstruction is consistent with most of the data observed.[73] Stein explains, that adding corroborative evidence always constitutes a new accuracy risk, so the "[a]cquisition of new information should be barred whenever it brings along an unacceptable risk of error".[74] It needs to be further examined, how to differentiate between acceptable and unacceptable risk of error in DF. Data of low quality, of unknown origin, or which source cannot be confirmed with the DF procedure must be excluded. It has the potential to erode any protection for innocent people given the risk of error and bias is very high and wrongful corroboration of such data might compromise even legitimate data.

44 Corroboration in DF is not only on data level, but also on methods and tools level. Accumulation of several DF methods and tools in time (periodically) or in the analytical perspective (heterogenous data analytics, data mining) could result in excessive interference with human rights (Art. 5, Art. 6, Art. 8, or Art. 10 ECHR)[75] and extraterritorial effects on the security of systems and devices.[76] Data access and collection legislations does not address legal questions of pre-processing, examination and analysis of data.[77] The availability of data for investigation should not result in very early pre-conceived assumption of guiltiness. Corroboration rules for error-mitigation can set a standard for databases quality and lawful processing of heterogenous data.

6. Summary

45 The table bellow summarizes the findings identified in this section asbuilding blocks of a PI-based techno-legal policy for digital evidence rules development. The policy can be further conceptualized and enriched with other fair trial principles and their interpretation and application in the digital evidence domain.

Table1. PI-based techno-legal policy for digital evidence.

PI-based evidence rule	Implication for DF evidence
Legal policy	
The PI has a function from the beginning of the criminal process to include safeguards in procedure with the bearing on the BoP.	– legal basis of DF method / tool – lawful use and purpose of DF method / tool – proportionality and legal justification of DF methods – oversight (not only judicial!)
Placing victims and offenders as active participants in the criminal process with rights, but also duties and responsibilities	– defence access to forensic aid – cross-examination of forensic report prior trial – right to explanation of DF method and results
Technology policy	
The PI is a procedural protection mechanism that requires integrity and accountability of the evidence production process	– reliability validation – documenting the logic of the processing in every stage of the evidence process
Protection from the negative risks of the investigation *PI-based error mitigation mechanisms*	– design of technology – machine and human error mitigation

IV. Conclusion and Further Work

Despite doctrinal, codification, and philosophical ambiguities, 46
the PI provides a rich theoretical framework for digital evidence regulation, international DF standards, and harmonized rules on the use of technology for investigative purposes. The PI is a procedural protection mechanism from the beginning of the criminal evidence handling and can be transposed to DF with a techno-legal policy. The PI requires safeguards for the BoP in the evidence process which can be satisfied with a legislative approach for establishing legal basis and purpose of DF methods and tools in combination with active defence forensics rights. PI-based evidence rules for integrity, accountability, and fair treatment show that the legislative approach must be complemented with technology policy based on legal reliability standard, validation of the logic of evidence processing, and PI-based error mitigation mechanisms. Further work requires the techno-legal policy to be translated and implemented in evidence processes and systems.

Radina Stoykova, PhD candidate

Marie Skłodowska-Curie Research fellow

University of Groningen, The Netherlands

Norwegian University of Science and Technology

radina.r.stoykova@ntnu.no

72 Eoghan Casey, 'Error, Uncertainty and Loss in Digital Evidence' (2002) 1 International Journal of Digital Evidence http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.77.9358&rep=rep1&type=pdf.

73 Fred Cohen, 'Toward a Science of Digital Forensic Evidence Examination' in Kam-Pui Chow and Sujeet Shenoi (eds), *Advances in Digital Forensics VI* (Springer 2010).

74 Ibid., Stein, p. 123.

75 See decision BVerfGE 112, 304 (12 April 2005) and commentary in Sabine Gless, 'Truth or Due Process? The Use of Illegally Gathered Evidence in Criminal Trials – Germany' [2010] SSRN Electronic Journal http://www.ssrn.com/abstract=1743530 accessed 10 August 2020.

76 Ryan Budish, Herbert Burkert and Urs Gasser, 'Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects' https://dash.harvard.edu/handle/1/36291726 accessed 19 September 2020.

77 Dennis Broeders and others, 'Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data' (2017) 33 Computer Law & Security Review 309.