Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations

Radina Stoykova

Department of Transboundary Legal Studies, Faculty of Law, University of Groningen, the Netherlands

ARTICLE INFO

Keywords:
Fair trial
Presumption of innocence
Equality of arms
Criminal investigation
Digital evidence
Reliability
Digital forensics

ABSTRACT

Digital evidence and digital forensics have a significant impact on criminal investigation. This requires an examination if the fair trial principle remains sound in the new domain.

In this paper the right to a fair trial in Art. 6 ECHR and its interpretation in case law is analysed in order to clarify its connection to evidence law and its specific application to the investigation stage of criminal proceedings. It is argued that the principle implicitly enshrines a framework for the development of universal evidence rules . Derived are two-groups of evidence rules: *equality of arms based* and *presumption of innocence based*. For each group specific challenges in the digital investigation are outlined and discussed in the context of a new governance model for digital evidence.

1. Introduction

Criminal investigations and trials have seen a fundamental change in recent years.[1] Given the digitalization of critical societal services and the increased use of digital devices by individuals, – the amount of available data related to human beings and their various actions and interactions has exponentially increased.[2] While these vast amounts of data may cause concerns about human rights, data protection, and security, their potential for efficient criminal investigations cannot be denied. For these reasons, digital evidence has become increasingly relevant in criminal proceedings and according to UK Chief Police Council "over 90% of all crime is recognized to have a digital element".[3]

Simultaneously, digitalization changes the methods, scope, and objectives of law enforcement work.[4] Gradually more computations are being used to deal with the volume and complexity of data born digital. The investigative stage of criminal proceedings becomes more pro-active,[5] complex,[6]

E-mail address: r.stoykova@rug.nl

[1] 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.

[2] Cisco Systems Inc. reported that on average each person will have more than 3 devices connected to IP networks by 2023, while in some countries like US and Japan the estimation is up to 11-13 devices per capita. Cisco Annual Internet Report (2018–2023) White Paper <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html> accessed 22 December 2021.

[3] The UK National Police Chiefs Council, 'Digital Forensic Science Strategy' (July 2020) 5. <https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf> accessed 22 December 2021.

[4] P Neyroud and E Disley, 'Technology and Policing: Implications for Fairness and Legitimacy' (2008) 2 Policing 226.

[5] 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.

[6] 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

https://doi.org/10.1016/j.clsr.2023.105801

volumized,[7] science-driven,[8] and outcome determinative.[9] This causes a significant disturbance in the traditional model of criminal justice,[10] which is reactive, personalized, and trial-centred.[11]

Such a disruptive change of a domain of such sensitivity with regards to fundamental human rights, foremost the right to a fair trial, may have led to the expectation of a comprehensively modernized legal framework around criminal proceedings to reflect this technological change and provide for new – adequate – safeguards. In reality, mostly selective changes to the legal framework have occurred – and only rather recently.[12]

Legal issues related to digital evidence are only partly addressed in most jurisdictions,[13] but there is a tendency to regulate at principle and supranational level, with a focus on law enforcement cooperation, rather than a fair-trial policy. At the Council of Europe (CoE) level, the adopted Second Additional Protocol to the Convention on Cybercrime[14] aims to enable cross-border access and exchange of digital evidence but does not seem to include any specific digital evidence, chain of custody or digital forensics standards. At the European Union (EU) level, proposed new mutual recognition instruments such as European Production and Preservation Orders do not include any provisions on ensuring reliability and contestability of digital evidence and has been put on hold for several years.[15] The newly propose Artificial Intelligence Act excludes from its scope international law enforcement cooperation,[16] which was heavily criticized by European data protection bodies.[17] Consequently, challenges with digital evidence governance not only exceed single jurisdictions but also the domain limitations of criminal procedure, digital forensics and evidence law, as they are rooted at the very intersection thereof.

This provokes a discussion as to what extent the investigative stage of criminal proceedings is sufficiently regulated in order to ensure accurate technology-assisted fact-finding, equal treatment of suspects, and protection of individuals from the adverse and prejudicial effects embedded in digital systems and data.[18] It also raises questions on the opportunity of the suspects, accused, and defendants to effectively access

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; Luca Caviglione, Steffen Wendzel and Wojciech Mazurczyk, 'The Future of Digital Forensics: Challenges and the Road Ahead' (2017) 15 IEEE Security Privacy 12.

[7] 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; Mark Scanlon, Xiaoyu Du and David Lillis, 'EviPlant: An Efficient Digital Forensic Challenge Creation, Manipulation and Distribution Solution' (2017) 20 Digital Investigation S29.

[8] Stephen Mason and Daniel Seng, Electronic Evidence (Fourth, University of London, Institute of Advanced Legal Studies 2017) para 2.15 <http://humanities-digital-library.sas.ac.uk/index.php/hdl/catalog/book/electronicevidence> accessed 18 January 2020; 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.

[9] 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/9781781007181/9781781007181.00016.xml> accessed 18 February 2020; Andrew Ashworth and Lucia Zedner, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure, and Sanctions' (2008) 2 Criminal Law and Philosophy 21.

[10] Ashworth and Zedner (n 9); Gil Rothschild-Elyassi, Johann Koehler and Jonathan Simon, 'Actuarial Justice' in Mathieu Deflem (ed), The Handbook of Social Control (John Wiley & Sons, Ltd 2019) <http://doi.wiley.com/10.1002/9781119372394.ch14> accessed 22 February 2021.

[11] Marks, Bowling and Keenan (n 1).

[12] 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); Martyna Kusak, 'Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters' (2017) 23 European Journal on Criminal Policy and Research 337; G Vermeulen, Wendy De Bondt and Y van Damme, EU Cross-Border Gathering and Use of Evidence in Criminal Matters: Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence? (Maklu 2010).

[13] United Nations Office on Drugs and Crime (UNODC), 'Draft Comprehensive Study on Cybercrime' (2013) ch 6 <https://www.unodc.org/e4j/data/_university_uni_/draft_comprehensive_study_on_cybercrime.html?lng=en> accessed 5 May 2021.

[14] Council of Europe, Cybercrime Convention Committee, 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-Operation and Disclosure of Electronic Evidence' (CM)57-final 2021). <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d> accessed 12.12.2021. Same developments on EU level - Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.COM/2018/225 final and additional Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM (2018) 226 final. Information note from the European Commission services following the stock-taking meeting with the US on an EU-US Agreement on cross-border access to electronic evidence, 26 March 2021 (Council document 7295/21, LIMITE, 31 March 2021).

[15] E. P., rapporteur Birgi Sippel, Legislative train (2021) <https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-cross-border-access-to-e-evidence-appointment-of-legal-representatives> accessed 16 December 2021.

[16] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final). See Art. 2(4).

[17] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

[18] Christian Chessman, 'A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution' [2016] SSRN Electronic

and examine digital evidence or challenge digital forensic expertise.[19] In addition, it seems that digital evidence challenges can neither be addressed from within national jurisdictions without a transnational framework, nor from within criminal procedure law or technological standardisation alone without interlinking both domains. To do so hereafter the digital evidence problematic is examined in the context of the fundamental principle of a fair trial.

This paper creates a conceptual framework which examines the continuous development of common principles of criminal procedure, based on Art. 6 ECHR and analyses those principles to demonstrate that they implicitly enshrine a framework for the development of universal evidence rules in the investigative stage of criminal proceedings.

The conceptual framework aims firstly to substantiate the connection between a fair trial at the level of principle, and the evidence law transposing it, without focusing on instrumental, jurisdiction-specific regulations on evidence. Therefore, each paragraph of Art. 6 is examined in the view of the European Court of Human Rights (ECtHR) to define the principles of criminal procedure specifically for the investigative stage and their relation to selected evidence rules. Secondly, the framework exemplifies challenges to the evidence rules in the digital forensic domain and the use of digital evidence by law enforcement in order to demonstrate the existence of shortcomings in these evidence rules. Lastly, cross-border evidence gathering and EU-specific mutual trust instruments for law enforcement cooperation are considered to have an amplifying effect on the identified challenges in the evidence rules. In this context, the development of a more adversarial and participatory model of investigation procedure is discussed.

2. The right to a fair trial and Art. 6 ECHR

The right to a fair trial is a universally recognized principle with a long-standing history in many jurisdictions' constitutional law, criminal procedure law and the case-law related thereto. At the transnational level, the right to a fair trial has been codified in the CoE (Council of Europe) European Convention on Human Rights (Art. 6 ECHR),[20] the UN (United Nations) Universal Declaration of Human Rights (Art. 10),[21] ICCPR (Art. 14) and EU Charter of fundamental rights (Art. 47).[22]

This paper will look at the right to a fair trial, and the principles contained therein, as a starting point to identify the challenges to a fair trial originating in the digital domain, thereby inspiring, together with seeking to balance the need for effective prosecution with individuals' rights, the further development of an approach to address such challenges.

Given the aim to propose a conceptual framework for digital evidence that (inter alia) seeks to overcome limitations from incoherent national jurisdictions, inspiration from the legal domain must be drawn from the transnational instruments codifying the right to a fair trial in a manner universally recognised across many jurisdictions. Of the four international instruments, Art. 6 ECHR, while not applicable globally but only in the 47 member states of the Council of Europe (CoE), is by far the most granularly developed codification in terms of case law and scholarly analysis. Conversely, of all granularly developed (national) codifications of the right to a fair trial, Art. 6 ECHR is the only one yielding a significant transnational territorial scope and recognition of its principles. It is therefore that we shall focus the following analysis on Art. 6 ECHR.

Art. 6 ECHR summarizes, non-exhaustively, the principles, individual procedural rights and additional safeguards which set a standard for procedural fairness and criminal procedure in accordance with the rule of law.

Art. 6 (1) sets the general principle of fairness, while Art. 6 (2) – the presumption of innocence – and Art. 6 (3) – list of minimum defendant rights – are "specific applications" of the principle.[23] The general principle of fairness allows theECtHR to examine whether the proceedings as a whole are fair, which surpass jurisdictional differences, and aim at developing common underlying principles of criminal procedure. The non-exhaustiveness of the specific aspects of the right to a fair trial allows the court to expand and develop new procedural guarantees in different contexts, which is consistent with the evolutionary principle of the ECHR as "a living instrument which must be interpreted in the light of present-day conditions".[24] This continuous development of common principles of criminal procedure based on Art. 6 ECHR implicitly enshrines a framework for the development of evidence rules – which are rules translating the Art. 6 ECHR principles into the handling of evidence in practice – and according to *Jackson and Summers* serves as "an ideal basis for […] cross-jurisdictional notion of procedural fairness".[25]

These evidence rules are of core interest to this paper as they substantiate the connection between a fair trial at the level of principle, and the evidence law transposing it, without focusing on instrumental, jurisdiction-specific regulations on evidence. They can therefore provide a first step towards a more granular view of the possible objectives of new international digital evidence governance model.

Analysing ECtHR case law underpinning these evidence rules, will be subject to two limitations in scope and method.

Firstly, the ECtHR has jurisdiction over potential violations of the fundamental human rights contained in the ECHR in cases referred to the Court, but not the underlying domestic

Journal <https://www.ssrn.com/abstract=2707101> accessed 16 November 2021.

[19] Christophe Champod and Joëlle Vuille, 'Scientific Evidence in Europe – Admissibility, Evaluation and Equality of Arms' (2011) 9 International Commentary on Evidence <https://www.degruyter.com/view/j/ice.2011.9.issue-1/1554-4567.1123/1554-4567.1123.xml> accessed 24 January 2021; Murphy (n 8).

[20] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

[21] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

[22] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[23] Deweer v. Belgium, no. 6903/75, 27 February 1980, § 56.

[24] Tyrer v. the United Kingdom, no. 5856/72, 25 April 1978, § 31.

[25] John D Jackson and Sarah J Summers, The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions (Cambridge University Press 2012) 80.

legal systems. Consequently, it takes a holistic approach to the overall fairness of the trial and its proceedings under a national legal system but will not perform a granular assessment of specific procedural rights in favour of affording a broad margin of appreciation to the national legal system from which a case originated. The ECtHR has upheld the position that the discretion on the assessment of admissibility, probative value, and burden of proof must be given to the specific national legal systems. Consequently, the Court does not act as a fourth instance examining admissibility or exclusionary rules on evidence but emphasises that evidence rules and procedures must mitigate procedural imbalances and afford protection for suspects and defendants against abuse of power by the state in general. Such an approach accounts for the dualistic nature of human rights as "both neutralizing and triggering the application of criminal law"[26] and implicitly, but not necessarily explicitly, develops evidence law and evidence procedural rules described by Roberts and Zuckerman as "foundational principles of criminal evidence".[27] It must therefore be part of this analysis to infer and conceptualise such evidence rules from the available ECtHR case law.

Secondly, the scope of the analysis of Art. 6 ECHR here concerns only its application to the investigative stage of the criminal proceedings. The Court has already outlined the increased complexity of investigations, and the resulting vulnerable position of suspects and accused at an early stage of the pre-trial.[28] The court emphasized that the fairness of the trial depends on the fairness of the pre-trial, and an initial failure to ensure fair trial safeguards during investigations can seriously prejudice the proceedings as a whole.[29] ECtHR has clarified that preliminary investigations and cross-border cooperation for evidence collection are covered by the procedural and material scope of the right to a fair trial. The procedural guarantees contained in Art. 6 are applicable not only when the suspect is formally charged with a criminal offence or arrested, but also at an earlier stage – "when preliminary investigations were opened", including when "the situation of the [suspect] has been substantially affected".[30] In other words, the procedural guarantees following from the right to a fair trial begin at a point in time which the Court decides on a case-by-case basis, and they include the moment when the investigation was directed at someone as a suspect, when the situation of the suspect is substantially affected, or when certain investigation measures such as searches begin.[31] In some cases, the protection is activated even earlier when a reasonable suspicion of guilt is formed.[32] Therefore, the case law can justify the conclusion that in principle the Art. 6 ECHR guarantees are invoked at the very beginning of the evidence processing procedure.

Further each paragraph of Art. 6 ECHR is examined in the view of ECtHR to define principles of criminal procedure specifically for the investigative stage and their relation to selected evidence rules. In this respect Art. 6 ECHR applications at a trial are only supportive and not examined. The stated challenges to the evidence rules in the digital forensics domain and the use of digital evidence by law enforcement are exemplary only in order to demonstrate the existence of shortcomings to these evidence rules originating from the specifics of the digital domain.

3. Extending Art. 6 ECHR to the investigative stage?

Fair trial safeguards apply throughout the whole criminal procedure as a continuous process, where the investigation might have a deterministic outcome or influence to a large extent the fairness of the trial.[33] The investigation is the stage of the proceedings where many of the digital forensic processes must be integrated into the criminal procedure. This integration should include processes and systems which validate factual accuracy regarding digital artefacts.

However, the ECtHR has always largely focused on the trial safeguards for evidence examination. The principle of orality, emphasised as an important safeguard at a trial, requires that the "evidence must be produced […again] in the presence of the accused at a public hearing with a view to adversarial argument."[34] The trial stage of the proceedings is where "the whole matter of the taking and presentation of evidence must be looked at in the light of paragraphs 2 and 3 of Art. 6."[35] Trial guarantees such as the principle of orality, disclosure and cross-examination have become increasingly ineffective in scrutinizing digital evidence.

The trial has as its main objective to examine the digital evidence presented in relation to the legal arguments of the case. Although the court can examine forensic reports or factual accuracy claims in relation to digital evidence, these might be extensive given the complexity and volumes of digital data. This has the potential to overburden the trial proceedings and to shift their objectives to validation and verification of complex processing operations, technology, and methods with all the inherent technological uncertainties and errors embedded in the process. The basic principles of equality of arms, public hearing, and presumption of innocence are challenged in criminal trials given the large amount of digi-

[26] F Tulkens, 'The Paradoxical Relationship between Criminal Law and Human Rights' (2011) 9 Journal of International Criminal Justice 577.

[27] Paul Roberts and AAS Zuckerman, Criminal Evidence (2nd ed, Oxford University Press 2010) ch 1.

[28] See Salduz v. Turkey, §§ 52 –54; Dvorski v. Croatia [GC], no. 25703/11, 20 October 2015, § 77; Ibrahim [GC], § 253.

[29] Engel and Others v. the Netherlands, no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72, 8 June 1976, § 91; Campbell and Fell v. the United Kingdom, no. 7819/77; 7878/77, 28 June 1984, §§ 95-99; Imbrioscia v. Switzerland, no. 13972/88, 24 November 1993, § 36.

[30] Eckle v. Germany, no. 8130/78, 15 July 1982, § 73 with reference to Deweer v. Belgium, no. 6903/75, 27 February 1980.

[31] Deweer v. Belgium, §§ 42-46; Ibrahim and Others v. the United Kingdom [GC], §249; Simeonovi v. Bulgaria [GC], no. 21980/04, 12 May 2017, § 110.

[32] Yankov and others v. Bulgaria, no. 4570/05, 23 September 2010, § 21.

[33] Saunders v. UK, no. 19187/91, 17 December 1996, § 74.

[34] Kostovski v The Netherlands, no. 11454/85, 20 November 1989; Barberà, Messegué and Jabardo v. Spain, no. 10590/83, 6 December 1988.

[35] Barberà v. Spain, § 78; also, Capeau v. Belgium, no. 42914/98, 13 January 2005, § 25.

tal data to be examined for accuracy. As stated by Ewald often both humans and software are challenged to have consistent analyses of the facts and "contradictions and misconceptions in judicial decisions about the facts of the crime"[36] are often observed. Furthermore, "[d]ecision making comes to be based on difficult-to-comprehend and low-quality data that is nonetheless treated as authoritative. Consequences include unclear accusations, unknown accusers, inversion of the onus of proof, and hence denial of due process."[37] This leads to the conclusion that the investigation should incorporate processes which can ensure factual accuracy and criminal procedure compliance for digital evidence. As it is, the results of the specialist digital forensics procedure cannot be fully presented in expert results reports or fully cross-examined by the judge or the defence during trial if a formal validation procedure is not performed and reported to the court. Considering also the ubiquitous and multipurpose use of digital evidence by law enforcement, a level of quality assurance should be established long before trial. Despite admissibility differences between jurisdictions, the requirement for reliability of digital forensics is turned into the main instrument for international discussion and harmonization of the investigative stage. This is supported also by the fact that many criminal investigations do not reach trial due to the increased use of plea bargaining and other settlements or confessions.[38] The suspect could be prosecuted very differently depending on the law enforcement agencies'digital forensics capabilities, the lack of protection for a formally – charged person, and being easily put in a position of having to prove her innocence.

In all cases the investigative stage can benefit from the implementation of evidence processing procedures which support more adversarial procedures by formal reliability validation processes or presumption of innocence by default design and use of technology. Such implementation of adversarial safeguards can ensure equal treatment of defendants and equal opportunity to contest the determinative stages of the evidence processing.

4. The fair trial principles as a source of evidence rules

4.1. *Inferring evidence rules – scope and method*

The ECtHR case law on Art. 6 ECHR (and the principles therein) allows for the inference of manifold evidence rules, which mandates for adequate structuring and scope limitations of this analysis to support focussing on the challenges particular to digital evidence. As a starting point, not least to facilitate interlinking this work with existing works, the principle structure provided by the Council of Europe's 'Guide on Article 6′ will be used, as it represents an essential analysis and categorisation of the ECtHR case law on Art. 6 ECHR.[39]

4.1.1. *The general guarantees*

Of the three *General Guarantees* laid down in Art. 6 (1) ECHR – *fairness, public hearing* and *reasonable time* – the latter two can be set aside as they do not face particular challenges in the digital investigation domain. The same applies to the *institutional requirements*, leaving the procedural requirements of the *General Guarantee* of *fairness* for primary focus.

The guarantee of *fairness* can be linked to the 10 principles contained therein following the structure suggested by the CoE:

- Effective participation in the proceedings,
- Equality of arms and adversarial proceedings,
- Reasoning of judicial decisions,
- Right to remain silent and not to incriminate oneself,
- (Requirements related to the) Administration of evidence,
- (Requirements related to) Entrapment,
- The principle of immediacy,
- Legal certainty,
- Prejudicial publicity, and
- (Requirements related to) Plea bargaining.

Of these ten principles, the *reasoning of judicial decisions*, the *principle of immediacy, legal certainty, prejudicial publicity* and (requirements related to) *plea bargaining* face only minor challenges rooted in the digital nature of digital evidence and shall therefore be set aside.

The principles of the *right to remain silent and not to incriminate oneself* and (the requirements related to) *entrapment* yield interesting challenges in the digital domain, such as protection of confidential information in digital forensics processing or the use of so-called 'honeypots' to attract and analyse cyber-criminal activity, but are of such a specific nature that they appear to be better addressed in works expressly focused on these specifics rather than this work aiming at universal standards for digital evidence.

Setting these principles aside, however, does not mean to ignore them, but rather not to centre further analysis thereon and to recur to these principles only contextually, where the subject-matter so requires.

The remaining three principles – *effective participation in the proceedings, equality of arms and adversarial proceedings*, and (requirements related to the) *administration of evidence* – are closely interlinked in the domain of digital evidence. Firstly, the possibility of *effective participation in the proceedings* directly delivers to establishing *equality of arms and adversarial proceedings*. Secondly, given that in the light of the complex digital forensic interplay involving multiple stages and expertise, all of which basically are accessible to the prosecution only, reliability risks become hard to trace and flawed digital evidence therefore will be hard to contest at trial without establishing standards on the *administration of evidence*. The latter becomes

[36] 'Big Data in Criminal Justice – Few Chances and Serious Risks' <http://videolectures.net/lawandethics2017_ewald_big_data/> accessed 16 March 2021.

[37] MR Wigan and R Clarke, 'Big Data's Big Unintended Consequences' (2013) 46 Computer 46.

[38] S Field, 'Fair Trials and Procedural Tradition in Europe', (2009) 29 Oxford Journal of Legal Studies 365; Boyne (n 9).

[39] Council of Europe, 'Guide on Article 6 of the European Convention on Human Rights - (Criminal Limb)' <https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf> accessed 12 December 2021.

a pre-condition to maintain *equality of arms* in view of digital evidence proceedings. Thirdly, all three aforementioned principles are supported by, and therefore intertwined with, the *Specific Guarantee* of *Defence Rights*, which in turn suggests treating all four holistically as one building block in the analysis aiming to infer evidence rules.

4.1.2. *The specific guarantees*

The *Specific Guarantee* of the *presumption of innocence* holds several fundamental principles. This paper provides only a general overview.

The CoE analysis categorises the *Specific Guarantee* of the *presumption of innocence* into five principles:

- (Protection against) Prejudicial statements,
- (Protection against) Adverse press campaigns,
- (Protection against) Sanctions for failure to provide information,
- The Burden of Proof, and
- (Protection against) Presumptions of law and fact.

The principle of (protection against) *Adverse press campaigns* does not yield particular challenges originating from the digital domain. (The protection against) *Sanctions for failure to provide information* is closely related to the *right not to incriminate oneself*[40] and shall be set aside for the same reasons.

The analysis shall therefore focus on evidence rules rooted in the principles of *burden of proof* as well as protection against *prejudicial effects*, rooted in the principles of (protection against) *prejudicial statements* and (protection against) *presumptions of law and fact*.

Based on the previous elaborations on the *equality of arms* principle, for the purposes of this paper the *defence rights* shall be treated holistically with that principle.

4.2. *Resulting scope and structure*

The analysis of inferred evidence rules and the challenges thereto in the digital domain can therefore be based on two primary building blocks: Firstly, the *equality of arms* principle jointly with the *defence rights*, and secondly the *presumption of innocence*.

4.3. *Evidence rules mapping overview*

To facilitate following the subsequent analysis of evidence rules inferred from the Art. 6 ECHR principles in the ECtHR case law, the derived evidence rules shall be briefly summarized here.

From the principles of equality of arms and adversarial proceedings in conjunction with defence rights the derived evidence rules are as follows:

- Possibility to challenge the evidence: fair disclosure of and to information about the evidence
- Time and facilities to prepare the defence evidence
- Maintaining equality of arms against technology-assisted expert evidence
- Fair procedure to evaluate the lawfulness and the lawful use of evidence
- Legal assistance at crucial stages of the evidence handling

From the presumption of innocence, the following additional evidence rules are derived:

- Accurate fact finding
- Protection against prejudicial effects in evidence procedure
- Protection against Reverse burden of proof
- Protection against coercive measures in evidence collection and processing
- Protection against presumption of fact

This work acknowledges that several of the evidence rules to be inferred are not necessarily in a strict many-to-one relation with regards to the principles contained in Art. 6 ECHR, but will often benefit adjacent principles in a many-to-many relation. It is for reasons of tangible structure and manageable complexity that inferring the evidence rules has been mapped to those principles which a particular evidence rule is most closely related to.

This work further acknowledges that more than the listed evidence rule could be inferred from the Art. 6 principles to be examined. However, as the purpose of this analysis is not to provide a comprehensive set of evidence rules, but rather to substantiate that the magnitude of unaddressed challenges originating from the digital nature of digital evidence mandates exploring a different approach for their implementation in the digital domain in general, focussing on a selection of evidence rules and the challenges related thereto will suffice to underpin this claim.

5. Equality of arms and defence rights based evidence rules

Art. 6 (1) ECHR encompasses two general principles of fair criminal procedure: the principle of equality of arms and the principle of adversarial proceedings. The equality of arms principle sets a general evidence rule that every party to the criminal proceedings must have "a reasonable opportunity to present his case in conditions that do not place him at a disadvantage vis-à-vis his opponent".[41] Given the need for effective prosecution, and given the very different nature of the roles of prosecution and defendant, full equality can never be realized at the investigative stage[42] and does not require the defence to be granted the same capabilities as the prosecution. Instead, the principle requires the investigative and evidence handling procedures to be designed in a way that will not introduce a procedural imbalance between the opposing parties.[43] The court requires equality between the opposing

[40] Ibid 74.

[41] Öcalan v. Turkey [GC], § 140; Foucher v. France, § 34; Bulut v. Austria.

[42] Stefan Trechsel and Sarah J Summers, Human Rights in Criminal Proceedings (Oxford Univ Press 2006) 96–98.

[43] Jackson and Summers (n 25) 84.

parties in their opportunity to present arguments and challenge the evidence[44] and equal participation of the defence and prosecution in proceedings examining evidence.[45]

The equality of arms and adversarial proceedings principles are complemented also by the general right of an accused to participate effectively in a criminal trial[46] and the specific defence rights enshrined in Art. 6 (3) ECHR. Art. 6 (3) (a) requires the defendant to have knowledge of the factual and legal basis of the charges against him,[47] while Art. 6 (3) (b) guarantees to the applicant "adequate time and facilities for the preparation of his defence".[48]

As there are overlaps and interdependencies between the general Art. 6 (1) and the specific principles in Art. 6 (3),[49] as demonstrated in Section 4.1, they are examined together to derive the five following evidence rules, which are also interpreted in relation to challenges arising from their application in the digital evidence domain.

5.1. *Fair procedure to evaluate the lawfulness and the lawful use of evidence*

Fair administration of evidence is a general principle of a fair trial. The evidence rule, which it encompasses ensures a fair procedure to evaluate the lawfulness and the lawful use of evidence.

5.1.1. *Case law analysis*

ECtHR does not focus on evaluating the admissibility of evidence under domestic law, but the procedural possibilities open to the defendant of contesting the way it is obtained and used.[50] National courts have a high level of discretion as to the admissibility and probative value of evidence. ECtHR addresses the following requirements to ensure a fair procedure: maintaining the ability to evaluate the quality of the evidence (i.e., verify "whether the circumstances in which it was obtained cast doubt on its reliability or accuracy."[51]); maintaining contestability (including ensuring the "opportunity of challenging the authenticity of the evidence and of opposing its use"); and compensation for reliability shortcomings by introducing supporting evidence (i.e., questionable evidence must be evaluated in the light of supporting evidence).[52]

As the lawfulness of obtaining the evidence and the lawful use of evidence depend on other Fundamental Rights, such as the right to respect for private and family life, home and correspondence (Art. 8 ECHR), providing the benchmark for "lawfulness", in the context of this evidence rule Art. 6 is interpreted in conjunction with the applicable other Fundamental Rights at stake. Consequently, the case law relevant to digital evidence will often enshrine a combined application of Art. 6 and Art. 8 ECHR. In essence, the Court evaluates firstly if a violation of another Fundamental Right results in unlawfully obtained evidence. Second an independent evaluation is required if the use of such evidence within the overall fairness of the proceedings would result in a violation of Art. 6 ECHR.

The greater the intrusiveness of the investigation measure and the power of the authority, the more the ECtHR observes which safeguards are in place to prevent abuse of power.[53] The fact that the Court evaluates the fairness of the proceedings as a whole means that some inconsistencies or breaches of procedure cannot automatically render the whole investigation unfair, but an accumulation of irregularities may do so. Breaches of legality are established always when the law or the proceedings fail to strike a balance between the rights of the defendant and the obligation for prosecution and successful conviction.[54] Often this relates to effective safeguards for the suspect at the pre-trial phase against intrusive investigation and proper documentation of the events related to evidence handling. The Court, for example, underlines the importance of greater scrutiny in "a preliminary investigation [...of the] methods used to obtain evidence for the prosecution"[55] and the examination of "any possible irregularities before the case was brought before the courts".[56]

The matter of intrusive evidence-gathering measures during an investigation requires both substantive and procedural quality evaluation.[57] The Court states that the law must indicate clearly the scope of the discretion conferred on the competent authorities and the manner of its exercise,[58] especially when the technology available for use is continually becoming more sophisticated.[59] It states that it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an *unfettered power*.[60] In *Khan* the Court held that intrusive surveillance techniques should be regulated by law and not by police guidelines, which are not sufficiently binding and do not meet requirements for foreseeability.[61] It further requires that the law and procedure are precise, and of sufficient quality to give the individual adequate protection against arbitrary interference.[62]

In the evaluation of the quality of the law the Court takes into consideration: the legal bases of the measure in view of the fair trial safeguards, focussing on aspects such as imminent danger, surveillance to be based on presented facts, time limits, authorization, notification after termination and super-

[44] Borgers v. Belgium and Zahirović v. Croatia, §§ 44-50.
[45] Zhuk v. Ukraine, no. 45783/05, 21 October 2010, § 35; Eftimov v. the former Yugoslav Republic of Macedonia, no. 59974/08, 2 July 2015, § 41; Ozerov v. Russia, no. 64962/01, 18 May 2010, §§ 53-55.
[46] Murtazaliyeva v. Russia [GC], no 36658/05, 18 December 2018, § 91.
[47] Pélissier and Sassi v. France [GC], no. 25444/94, 25 March 1999, § 51; Kamasinski v. Austria, no. 9783/82,19 December 1989, § 79.
[48] Leas v. Estonia, no. 59577/08, 6 March 2012, § 80
[49] Council of Europe (n 39).
[50] Lee Davies v. Belgium, no.18704/05, July 28, 2009, §§40-54
[51] Dragojević v. Croatia, no. 68955/11, 15 January 2015, § 129.
[52] Prade v. Germany, no. 7215/10, 3 March 2016, §§ 34-35.
[53] Klass and Other v. Germany, no. 5029/71, 6 September 1978; Malone v. UK, The United Kingdom, no. 8691/79, 2 August 1984; Kruslin v. France, no. 11801/85, 24 April 1990.
[54] Jalloh v. Germany [GC], no. 54810/00, 11 July 2006, § 97; Prade v. Germany, cited above, § 35.
[55] Hulki Güneş v. Turkey, no. 28490/95, 19 June 2003, § 91.
[56] Miailhe v. France (No. 2), no. 18978/91, 26 September 1996,§ 43.
[57] Malone v.the UK, cited above; Huvig v. France, no. 11105/84, 24 April 1990; Kruslin v. France, cited above.
[58] Malone v. the UK, § 87.
[59] Kruslin v. France, § 32.
[60] Malone, § 68.
[61] Khan v. the United Kingdom, no. 35394/97, 12 May 2000, § 27-28.
[62] Malone v. the UK, § 68, Huvig v. France, § 29.

vision for notification.[63] More importantly, procedural requirements refer to the procedure to be followed for *examining, using and storing the data obtained*; the precautions to be taken when *communicating the data to other parties*; and the circumstances in which recordings may or must *be erased or destroyed*.[64] The court emphasizes clear procedures for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the *recordings intact and in their entirety* for possible *inspection by the judge* (who can hardly verify the number and length of the original tapes on the spot) *and by the defence*.[65]

Apart from these procedural guarantees for quality of law and procedure, the court did not develop further criteria to examine the prejudicial effects of illegal acts compromising data integrity, the impact of questionable forensic techniques on the investigative process or the adverse effects of illegal access and data collection on the presumption of innocence (PI) principle.

Human rights scholars discuss two criteria for the evaluation of illegally obtained evidence relevant to the digital context.[66] The first criterion is examining whether the evidence is of sufficient quality or the illegality of the collection amounts to questionable reliability. When the reliability of the evidence as such is not hampered by the illegal act of obtaining it, the second criterion is related to the investigation's integrity and its compliance with the rule of law as the ultimate tests for fairness at the investigative stage.[67]

In *Schenk*[68] the Court made a judgement on illegally intercepted calls in France handed over to the Swiss law enforcement authorities. Although ECtHR acknowledged the problem with interception without a legal basis, it concluded nevertheless that there was no violation of Art. 6 ECHR and in particular that in the view of other evidence the illegal interception did not amount to treatment of the suspect as guilty before conviction (applying the PI principle in addition).

Since *Schenk* the ECtHR has established case law where the evidence obtained in violation of Art.8 was considered admissible, when the accused had the possibility to *contest the authenticity and quality of the evidence* and when such evidence *is not the only (or main) evidence, on which the conviction is based*.[69] Both of those arguments are problematic. Arguably, the prosecution is the party which needs to prove the authenticity and quality of the evidence. *Jackson and Summers* argued that "where there has been a failure by the prosecution to obtain significant evidence or undertake various tests to establish the accused's guilt, the burden ought to be placed on the prosecution to prove why that has not prejudiced the defence".[70] This obligation must not depend on the defence's ability to challenge on relevant grounds (as it risks reversing the burden of proof). The defence has the opportunity to present legal arguments against the use of incriminating evidence, but it is ill-suited to raise claims on the (factual) accuracy of the fact-finding. Therefore, four of the judges in *Schenk* expressed disagreement in stating that no "court can, without detriment to the proper administration of justice, rely on evidence which has been obtained not only by unfair means but, above all, unlawfully."[71] Later in *Doorson*, the Court acknowledged that its task is "to ascertain whether the proceedings as a whole, *including the way in which evidence was taken*, were fair."[72]

The second condition, requiring the prosecution to provide supporting evidence in addition to the illegally obtained evidence, was abandoned in *Khan*, where the Court gives importance only to the reliability standard, stating that "[w]hile no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker".[73] The *Khan* decision was broadly criticized[74] as the only one where although there was no legal basis for the surveillance measures and therefore the main evidence, on which the conviction was based, was obtained in violation of Art.8, no violation of Art. 6 ECHR was found.

In *Allan* the Court deviated from the *Khan* judgement and held that when main evidence is obtained through psychical coercion it violates the privilege against self – incrimination.[75] In further rulings the *Khan* decision's lower standards for lawfulness of obtaining evidence were repeated,[76] nevertheless the court also emphasized the additional requirement for supporting evidence.[77] In *Seton* the Court pointed out the importance of corroborating evidence in cases where procedure fairness and the principle of orality are disputed, stating that the "use as evidence of absent witness's telephone recording did not make the trial unfair in view of other decisive evidence".[78]

It appears that the contradiction between the *Schenk* and the *Khan* decisions on supporting evidence has not been resolved unambiguously so far; however, the number of Art 8 violations during investigations is growing and the court does not state any criteria to address that increase and its grow-

[63] ibid., Klass v. Germany.
[64] See Huvig, § 34; Amann v. Switzerland [GC], no. 27798/95, 16 February 2000, §§ 56-58, ECHR 2000-II; Prado Bugallo v. Spain, no. 58496/00, 18 February 2003, § 30. Emphasis mine.
[65] See Huvid. v. France, § 34. Emphasis mine.
[66] Mireille Delmas-Marty and John R Spencer (eds), European Criminal Procedures (1st pbk. ed, Cambridge University Press 2005) ch 11; Jackson and Summers (n 25) chs 6–8; Roberts and Zuckerman (n 27) chs 5–7.
[67] Delmas-Marty and Spencer (n 66) 603.
[68] Schenk v. Switzerland, no. 10862/84, 12 July 1988.
[69] Schenk v. Switzerland, no. 10862/84, 12 July 1988, §§ 46-48 and P.G. and J.H v. the United Kingdom, 44787/98, 25 September 2001, §§ 78 –79.
[70] Jackson and Summers (n 25) ch 11.
[71] Dissenting opinion of Judges Pettiti, Spielmann, de Meyer and Carillo Salcedo in the Schenk case.
[72] Doorson v. the Netherlands, no. 20524/92, 26 March 1996, § 67. Emphasis mine.
[73] Khan v. the United Kingdom, no. 35394/97, 12 May 2000, § 37; Boykov § 90.
[74] Roberts and Zuckerman (n 27) 202. with reference to Ashworth calling it one of "the least impressive examples of Strasbourg jurisprudence".
[75] Allan v. the United Kingdom, no. 48539/99, 5 November 2002, § 52.
[76] Heglas v Czech Republic, no.5935/02, 1 March 2007, §§ 68 and 75–76 and Chalkley v. the United Kingdom, no. 63831/00, 12 June 2003.
[77] Ibid., 25, compare §§ 129 and 133.
[78] Seton v. the United Kingdom, no. 55287/10, 31 March 2016.

ing impact on the right to a fair trial. Nevertheless, the ECtHR elaborated that in cases where the evidence is in question, "the existence of fair procedures to examine the admissibility and test the reliability of the evidence takes on even greater importance."[79] While the court does not have competence to further elaborate those principles with respect to concrete evidence procedures under the fourth-instance limitation, this view supports the approach to put the reliability of digital evidence into focus and to address it with a framework of reliability standards.

5.1.2. *Challenges in the digital domain*

The requirement for fair procedures for testing the evidence's reliability and completeness is challenged in the digital evidence domain as law enforcement and the lawfulness-related questions of how digital evidence is obtained and processed (e.g., scope, authorisation, safeguards) is conveniently disguised under layers of computer-facilitated operations and human-machine interactions. Currently there is an over-emphasis both by scholars and legislators on access and collection of data through technology, while further steps in data processing, specifically the legal compliance of preprocessing, examination and analysis of data[80] from different sources in a law-enforcement context is not addressed in any legislative initiative. It is also unclear how information inferred from data (analytics) can be protected and used during the investigation.

It is questionable if the defence (and in some cases the judge) have a sufficient possibility to contest the authenticity and quality of the digital evidence by the prosecution. This safeguard cannot be realized if data processing is not sufficiently documented to establish the evidence origin, acquisition, examination, and analysis. In relation to exculpatory evidence, the defence has a heavy burden to prove the exact scope and location of the digital data, or the particular importance of the requested digital evidence to the case and is not clear if and how to implement defence rights in stages like examination and analysis of evidence. The underlying issue is the lack of procedures to verify and validate the evidence processing at all stages, where technical and legal challenges emerge in establishing chain of custody, data integrity, attribution, and reliability of forensic methods and tools in the digital investigation.

A second group of challenges is related to the fact that innovative digital forensic methods and tools for evidence processing might be kept secret by law enforcement. This might be related to the tool and method used, the processing operations, or the resulting digital evidence itself. This could result in the use of alternative explanations for how evidence was found, a practice known as a parallel construction of evidence, or increased requests for non-disclosure of evidence with an intelligence or unknown origin.[81]

The identified problems with lawfulness and lawful use of evidence are amplified in cross-border evidence gathering given the danger of evidence forumshopping. Digital data can be copied without degradation and irrespective of jurisdiction. If one country prohibits certain intrusive investigative measure, LEAs can use mutual assistance or mutual recognition instruments in order to acquire evidence from a country where such a measure is lawful. There is still no principle legislative approach to foreign evidence and national jurisdictions where countries have diverse laws on the use of foreign evidence[82] and apply less rigorous tests for its lawfulness. Consequently, the defence might lack an effective remedy to scrutinize foreign evidence while prosecution services are embedded in "formal trans-border networks which help them to find the best place to prosecute a case".[83]

Equality of arms could also mean that "both sides are denied something that might have been useful".[84] For example, the Court held that the equality of arms principle is upheld when both the prosecution and the defence could not benefit from evidence that has been lost and the trial court did not examine.[85] Responsibility of the prosecution for tampering or destroying digital evidence relevant for the defence is an open question though.

5.2. *Possibility to challenge evidence: fair disclosure of and information about evidence*

The principle of equality of arms and adversarial proceedings requires that "both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party".[86]

5.2.1. *Case law analysis*

The principle creates an obligation for the prosecution to disclose to the defence all material evidence in their possession for or against the accused[87] and a broader right to the defence to be presented with not only evidence directly relevant to the facts of the case, but also other evidence that might relate to the admissibility, reliability, and completeness of the former.[88]

[79] Allan v. the United Kingdom, § 47; Bykov v. Russia [GC], 4378/02, 10 March 2009.

[80] 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.

[81] Iris Wagner, 'Parallel Construction: Building Criminal Cases Using Secret, Unconstitutional Surveillance' (Criminal Legal News, 2018) <https://www.criminallegalnews.org/news/2018/may/14/parallel-construction-building-criminal-cases-using-secret-unconstitutional-surveillance/>; Human rights watch, 'US: Secret Evidence Erodes Fair Trial Rights Government Hides Investigative Methods from Accused' (2018) <https://www.hrw.org/news/2018/01/09/us-secret-evidence-erodes-fair-trial-rights>.

[82] Sabine Gless, 'Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial: Approaches to a General Principle', (2013) 9 Utrecht Law Review 90.

[83] Neil Boister, An Introduction to Transnational Criminal Law, Second edition, Oxford University Press 2018, para 17.10.

[84] Trechsel and Summers (n 42) 96.

[85] Jasper v. the United Kingdom [GC], no. 27052/95, 16 February 2000, § 57.

[86] Brandstetter v. Austria, no. 11170/84; 12876/87; 13468/87, 28 August 1991,§§ 66-67; Rowe and Davis v. the United Kingdom, no. 28901/95, 16 February 2000, § 60; Fitt v. the United Kingdom [GC], no. 29777/96, 16 February 2000, § 44; Matanović v. Croatia, no. 2742/12, 04 April 2017; and Kobiashvili v. Georgia no. 36416/06, 14 March 2019.

[87] ibid. Fritt v. UK, § 44.

[88] Rowe and Davis v. the UK, cited above, § 66; Mirilashvili v. Russia, no. 6293/04,11 December 2008, § 200; Leas v. Estonia, cited

In relation to the burden of proof, the Court has stated that the prosecution has a positive obligation to investigate and collect evidence in favour of the accused[89] and to enable the defence to cross-examine witnesses against her.[90]

The right to disclosure of evidence is not an absolute right and can be limited. Judges have a broad discretion to limit access to evidence in order to protect other public interests such as national security, the need to protect witnesses at risk of reprisals or to keep police methods of crime investigation secret.[91] However, in such circumstances, the ECtHR insists that sufficient information must be provided to the judge in order to take an informed decision on non-disclosure.

Such exceptions must be limited to what is strictly necessary and any difficulties caused to the defence by a limitation of its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities.[92] The strict necessity test for non-disclosure and the established restrictions on the use of other forms of secret evidence suggest that any non-disclosure will only be compatible with the "adversarial" requirement so long as that piece of evidence is not used to a decisive extent to form a basis for the conviction[93] or is not a crucial piece of evidence in the case.[94] The judge must be able to ensure that the facilities necessary for the preparation of the defence are not limited by the undisclosed material.

Art. 6 ECHR infringements occur where disclosure is refused of evidence that:

- has an important bearing on the charges held against the applicant,[95]
- was used and relied upon for the determination of the applicant's guilt, or
- it contained such particulars that could have enabled the applicant to exonerate her- or himself or have his or her sentence reduced with regard to the charges held against him or her.[96]

However, the Court clarified that if the evidence at issue is related to sensitive information the accused may be expected to give specific reasons for his request and the national judge enjoyed a wide margin of appreciation in deciding on the disclosure.[97] It must be noted that the specific reasons for access to surveillance files does not require arguments on the lawfulness of the surveillance operation, but reasoning on the importance of the content of such files to facilitate the defence standpoint. The Court acknowledged that legitimate reasons for a disclosure request for surveillance materials can be related to cross-examination of the lawfulness of the measure and the opportunity to choose evidence from the surveillance file.[98]

In *Mirilashvili*, the Court had to examine a situation where the governmental authorities refused the disclosure of materials relevant to the authorization of the wiretapping, because they were "related to the operational and search activities" of the police and national security secrets.[99] The ECtHR considered the defence to have a legitimate interest to access the materials and evaluated further whether the non-disclosure was counterbalanced by adequate procedural guarantees by the judicial authorities. The court concluded that the *ex parte* hearing in front of the military court judge failed to strike a balance between the public interest in non-disclosure and the importance of the documents to the defence. Particularly problematic was the fact that the military court accepted the blanket exclusion of all the materials from adversarial examination and the judge. The limited and vague decision on non-disclosure did not satisfy the balancing test because the judge did not examine *the content of the secret documents*, did not specify the reasons for non-disclosure, and the nature of the undisclosed materials. Blank reference to the secrecy of surveillance materials are general observations, while clear reasons for denying access[100] and evaluation of the importance of the undisclosed material and its use in the trial[101] are required. By contrast, in the cases of *Fitt* and *Jasper* the judge examined the withheld material and reasoned with respect to the defence interests, the defence was kept informed and was permitted to make submissions and participate in the decision-making process.[102] The court also states that in the light of "the principle of presumption of innocence and the defendant's right to challenge any evidence against him, a criminal court must conduct a full, independent, and comprehensive examination and assessment of the admissibility and reliability of evidence pertaining to the determination of the defendant's guilt, irrespective of how the same evidence may have been assessed in any other proceedings."[103]

ECtHR case law endorses closer and more rigorous examination of invasive evidence-gathering methods during inves-

above, § 81; Matanović v. Croatia, § 161; Windisch v. Austria, no. 12489/86, 27 September 1990, § 28; see also Dowsett v. the United Kingdom, no. 39482/98, 24 June 2003, § 41.

[89] V.C.L. and A.N. v. the United Kingdom, nos. 77587/12 and 74603/12, 16 February 2021, §§ 195-200.

[90] Trofimov v. Russia, no. 1111/02, 4 December 2008, § 33 and § 67; Cafagna v. Italy, no. 26073/13, 12 October 2017, § 42.

[91] Rowe and Davis v. the UK, cited above, § 61. Edwards and Lewis v. the United Kingdom, nos. 39647/98 and 40461/98, 27 October 2004, § 46.

[92] Doorson v. the Netherlands, § 72, and the Van Mechelen and Others, nos. 21363/93, 21364/93, 21427/93 and 22056/93, 23 April 1997, § 54.

[93] Doorson v. the Netherlands, §§66-83; Pesukic v. Switzerland, no. 25088/07, 6 December 2012.

[94] Georgios Papageorgiou v. Greece, no. 59506/00, 9 May 2003, §§35-40.

[95] Rowe and Davis v the UK, cited above, § 66; Korellis v. Cyprus, no. 54528/00, 7 January 2003, §§ 33-35; and Mirilashvili v. Russia, no. 6293/04, 11 December 2008, § 199.

[96] C.G.P. v. the Netherlands, no. 29835/96, 15 January 1997.

[97] Mirilashvili v. Russia, cited above, §§ 201-202; Bendenoun v. France, no. 12547/86, 24 February 1994, § 52; Natunen v. Finland, no. 21022/04, 31 March 2009, § 43; Janatuinen v. Finland, no. 28552/05, 8 December 2009, § 45; and Leas, cited above, § 81

[98] Matanović v. Croatia, cited above.

[99] Mirilashvili v. Russia, cited above, § 201.

[100] Leas v. Estonia, no. 59577/08, 6 March 2012, §87.

[101] Jasper, cited above, §§ 54-55.

[102] Fitt v. the United Kingdom [GC] § 46 and Jasper, cited above, § 53.

[103] Belugin v. Russia, no. 2991/06, 26 November 2019, § 68 and Huseyn and Others v. Azerbaijan, nos. 35485/05 and 3 others, 26 July 2011, § 212.

tigation[104] and greater procedural rights protection for suspects at the pre-trial phase, especially the access to and further search for evidence.[105]

5.2.2. *Challenges in the digital domain*

Complex issues with the right to disclosure arise from the vast amount of information to be processed in order to identify relevant evidence and the dominant position of the prosecution which is in possession not only of the data but also of the technology required to examine it.[106]

The ECtHR case *Rook* vs. *Germany* shows the struggle by criminal justice systems to balance the fair trial safeguards and the need for effective prosecution in digital evidence procedures and with respect to digital forensics technology. The bribery investigation against Rook resulted in 78,970 telecommunication data sets and *14 million* electronic files acquired and imaged by digital forensics examiners. Given this overwhelming data set, the first question of legal importance was whether the prosecution and the defence had the opportunity, time, and resources to identify the relevant elements for the case data. The prosecution used digital forensics data-analysis tools to identify only 28 telephone conversations and 1100 files as relevant to the case. During the investigation the defence lawyer was provided with access only to the relevant files printed on paper and was denied access to lists indicating the raw data from the various telephone lines. After the indictment, the prosecution gave access to the decrypted, imaged data on hard drives provided by the defence. Beyond the principal question of access, which also triggers questions in view of the selected evidence as the non-selected data sets might contain exculpatory evidence, several other issues arise. Firstly, the effectiveness of presenting (large amounts of) paper printouts (non-searchable by automated means) is an obsolete practice and does not allow the effective participation of the defence in the digital evidence examination. Secondly, data copying, and exchange might not only introduce data tampering or destruction, it could also be time-consuming. Moreover, in order for digital evidence to be contested on meaningful grounds the defence must have access not only to the data set or the data content, but also to the chain of custody and integrity preservation information, which exposes system design and technology problems as well.

In Rook, ECtHR endorsed the view that disclosure pre-trial is necessary given the volumes and complexity of the data. However, the court felt that the prosecution did not comply fully with the equality of arms principle and with the defendants' rights because: 1. it did not provide a list of raw data material at an earlier stage of the investigation; 2. did not grant access for the defence to the data-analysis tool used; 3. did not specify search parameters in order to justify and disclose the logic for the identified relevant data. Despite these limitations of procedure, the Court held that there was no violation of Art. 6 (1) ECHR. In *Barberà* the Court ruled that "1600 pages investigation file, the bulk of which did not concern the defendants"[107] does not meet the disclosure requirement. It was required that the prosecutor specify in detail the particular evidence on which he based his account of the facts as well as disclosure of exculpatory evidence and unused material.

In this case and in relation to another, the court established two procedural safeguards for the defence – namely the defence to have the opportunity: *(i)* to be involved in the definition of the criteria for determining what may be relevant[108] and *(ii)* to conduct further searches for exculpatory evidence.[109] It would appear that the court emphasises that digital forensics processing should be done in a way which demonstrates how relevant digital evidence is discovered. However, it remains unclear whether each processing step in evidence acquisition, examination, and analysis should be accountable, or only the results of the processing.

It is unclear why the Court considers that the search for exculpatory evidence should be limited only to data identified as relevant by the prosecution, and not to the whole data set. Another questionable point is that the court mentions the need for judicial supervision of the process of selection of relevant data, but it is unclear if this is a cumulative or alternative safeguard in respect to defence participation. Arguably, judicial oversight as a cumulative requirement might be necessary a) where there is disagreement as to the scope and relevance of additional searches requested by the defence or b) where the data set contains sensitive or confidential information, or c) where the prosecution relies on secret or sensitive data for evidence. This was endorsed in the Court decision in relation to protection of confidential information during digital investigations.[110] The court does not elaborate how the identification of relevant and exculpatory evidence should be technically or procedurally facilitated. A better solution might be to appoint digital forensic examiners to a specific proceeding to whom both prosecution and defence can address their hypotheses and queries. The judge is best prepared to decide to what extent those requests can be granted, *after* the evaluation of the available data, digital forensics methods and digital forensics technology conducted by the digital forensics examiner. This, however, requires that the digital forensic tools, methods, and processes are sufficiently understood by all parties to the proceedings and that they are sufficiently documented for audit and use on trial. It would benefit, moreover, from a standardisation framework, to tackle specific technologies such as artificial intelligence models for evidence analysis and the corresponding procedural safeguards. This might require a different interpretation of existing, and the introduction of new, evidence rules applicable to the investigation to satisfy those initial ECtHR consideration on digital evidence disclosure.

5.3. *Time and facilities to prepare the defence evidence*

A more abstract interpretation of the two cases of *Rook v. Germany* and *Sigurður Einarsson and Others v. Iceland* raises

[104] Malone v. the UK, Huvig v. France and Kruslin v. France, cited above.
[105] S. v. Switzerland.
[106] Sigurður Einarsson and Others v. Iceland and Rook v. Germany, no. 1586/15, 25 July 2019.
[107] Barberà v. Spain, § 77.
[108] Sigurður Einarsson and Others v. Iceland, no. 39757/15, 4 June 2019, § 90; also Rook v. Germany, no. 1586/15, 25 July 2019, §§ 67 and 72.
[109] Sigurður Einarsson and Others v. Iceland, § 91.
[110] Saber v. Norway no 459/18, 17 December 2020.

broader questions related to the general principle that the defence should have the ability to put all relevant defence arguments before the court.[111] From this principle of the evidence rule for providing *time and facilities to prepare defence evidence* can be derived.

5.3.1. *Case law analysis*

Art 6 (3)(b) requires adequate time for the inspection of a file[112] and the opportunity for obtaining copies of relevant documents from the case file.[113] For example, in one case the Court held that five days to examine a 1500 page case file is sufficient time to prepare the defence[114] since the defendant and his two lawyers had time to analyse the file in detail, and that the applicant had not been limited in the number and duration of his meetings with the lawyers. In the *Rook* case the ECtHR also found no violation of Art. 6 (3) (b) ECHR since it considered that three and a half months were sufficient time for the defence to prepare its case based on the data provided. It is, however, noticeable that both cases relate to the exponential amount of data to be examined by the defence and the increasing time for preparation.

5.3.2. *Challenges in the digital domain*

In the near future the access to expensive data-examination tools might be required in order not to overburden the disclosure process. Even if the defence is granted access to forensic tools, the defence lawyer is ill equipped to perform an expert digital forensic examination and analysis of data sets, which are not one-click-solutions but require in-depth knowledge of and experience with digital forensics methodology. In general, the preparation of the defence and the disclosure process can become overburdened as the defence can hardly verify the number and length of the original data sets and the resulting findings on the spot, which leads to increased time and resources for evidence data handling. Of crucial importance is the access to the chain of custody, knowledge of the processing operations at each stage, and accountability information in order to access the legality and proportionality of the investigation measure, the scope of authorization, and the reliability of the evidence.

This situation might require completely new evidence procedures related to early disclosure; defence forensic aid to prepare digital evidence; examination of digital forensic procedure, methods and tools; justification and explanation of search parameters to identify relevant data; a right to participate in the examination and to confront the expert and the data-analysis tool results; and a responsive disclosure of decrypted information in investigations. In addition, digital evidence is the result of a specialist digital forensic procedure which cannot be fully presented in the expert results reports or fully cross-examined by the judge or the defence during trial if a formal validation procedure is not performed and reported to the court.

The evidence rule for time and facilities for defence evidence also protects the accused against speed trials,[115] where efficiency is prioritised at the expense of defence rights. In technology-facilitated evidence processing this might have implications as to the extent to which the digital forensics examiner can examine hypotheses about the origin of the data discovered, and as to the search for relevant data being sufficient to conclude. Likewise, very lengthy proceedings where the investigation and the trial are spread across several years might lead to a need to prove secure storage of evidence, or to obsoletion of digital forensics tools and methods.

It follows that the examined deficits in the expert evidence evaluation procedures are amplified in the digital evidence domain where, as of now no universal standards for the application of methods and technology exist. The ECtHR does not, and by competence cannot, develop a framework which can ensure that unreliable, exaggerated, or misleading expert evidence will be scrutinized sufficiently both by the judge and the defence. The scientization and digitalization of criminal investigations in recent years will require a more robust approach in this aspect. *Vuille* argues that the ECtHR must be competent on such matters and that they must be addressed at a supra-national level in order to avoid different treatments of evidence and suspects, and considering that an important proportion of convictions is based at least in part on evidence of a scientific or technical nature while national legislation on expert evidence matters remains of low quality and very diverse.[116] The efficiency of such evidence procedural rules will depend on the design of evidence platforms that can implement digital forensic standards and automate compliance. These findings underpin the need to develop a framework for reliability standards as a possible approach to address these challenges.

5.4. *Maintaining equality of arms against expert evidence*

The principle of equality of arms is interpreted as a requirement for equal treatment of the parties in similar procedural situations. The ECtHR case law establishes the evidence rule that witnesses for the defence and for the prosecution be treated equally. In the digital domain this rule gains momentum, as the equality of arms principle is considered important with respect to the appointment of court experts,[117] who can access and interpret digital evidence according to digital forensics standards.

[111] Gregačević v. Croatia, no. 58331/09, 10 July 2012, § 51.
[112] Huseyn and Others v. Azerbaijan, § 174- 178; Iglin v. Ukraine, no. 39908/05, 12 January 2012, §§ 70-73.
[113] Rasmussen v. Poland, no. 38886/05, 28 April 2009, §§ 48-49; Moiseyev v. Russia, no. 62936/00, 9 October 2008, §§ 213-218; Matyjek v. Poland, no. 38184/03, 24 April 2007, § 59; Seleznev v. Russia, no. 15591/03, 26 June 2008, §§ 67-69.
[114] Lambin v. Russia, no. 12668/08, 21 November 2017, §§ 43-48.
[115] OAO Neftyanaya Kompaniya Yukos v. Russia, no. 14902/04, 31 July 2014, § 540; Borisova v. Bulgaria, no. 56891/00, 21 December 2006, § 40; Malofeyeva v. Russia, no. 36673/04, 30 May 2013, § 115; Gafgaz Mammadov v. Azerbaijan, no. 60259/11, 15 October 2015, §§ 76-82.
[116] 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.
[117] Bönisch v. Austria, no. 8658/79, 2 June 1986, § 32 and Brandstetter v. Austria, § 45.

5.4.1. *Case law analysis*

As the ECtHR is attentive to the fact that expert opinion is likely to have significant weight in the Court's assessment of the issues within that expert's competence,[118] the Court requires effective procedural measures to test the expert evidence's credibility and reliability and take into consideration the position occupied by the experts throughout the proceedings, the manner in which they performed their functions and the way the judges assessed the expert opinion. Although the Court clearly states that the defence is not entitled to counter the expertise,[119] the procedural rules must not deprive the defence of challenging expert opinion effectively when this requires specialist knowledge.[120]

Even though the digital forensics problematic is relatively new, the ECtHR has established the relation between the equality of arms principle and expert evidence in older cases, which are relevant by analogy. The defence has the right to participate in the expert examination[121] and to confront the expert witness.[122] This means that the defence must have an opportunity to effectively contest and comment on the expert's findings,[123] and to be presented with the expert report as well as the expert findings on exculpatory evidence.[124] The Court states that an important counterbalancing factor in the assessment of the overall fairness of the proceedings is the opportunity to scrutinize the expert report and documents by an expert instructed by the defence.[125] However, the defence has no right to counter expertise[126] and it is at the national judge's discretion to refuse expert testimony[127] according to the principle of procedural economy. The burden of proof is on the defence to *justify objectively* that a second expert opinion is needed.[128] This is a rather stringent requirement for the defence. In the *Mantovanelli* case the Court found a violation of Art. 6 ECHR stating that the opportunity to comment effectively on the reliability of the expert evidence includes not only the opportunity to be present at expert interviews, but also to access the full documentation on which the expert report was based.[129] The case indicates that ECtHR is in favour of involvement of the defence at an earlier stage of the forensic examination. Moreover, in cases where the sole and decisive expert evidence came from the prosecution the Court found a violation of the equality of arms principle.[130]

There are noticeable inconsistencies in the ECtHR case law on digital forensic evidence. In relation to physical evidence, in *Zahidov* the Court decided that procedural inaccuracies related to time lapses between arrest and searches, improper or missing documentation, breach of the defendant's rights to examine the search video recording, or the absence of a lawyer during interrogation amounted to circumstances which cast doubt on the reliability.[131] Moreover, the authenticity of the evidence and challenging its use was considered as a separate question for evaluation.[132] It should be argued that unlike physical, digital evidence is much more volatile given the known digital evidence dynamics,[133] and the requirements for reliability and authenticity must be reinforced and more elaborate.

In the *P.G. case* the ECtHR did not engage in any discussion about the reliability and authenticity of the digital evidence, even though there was such an opportunity since "the evidence in relation to at least the first applicant was not particularly strong in that the forensic expert was only able to conclude that it was '*likely*' that his voice featured in the tape recordings."[134] This lack of a reliability evaluation is problematic given the fact that often national courts take the reliability of expert opinion as granted, while the defendant's stand is considerably weaker to challenge expert opinion.[135] Another difference from the considerations of physical evidence is that in respect of digital evidence the court did not make any comments on the provenance and chain of custody documentation, which is crucial to evaluate the legality of the police act in obtaining the evidence and establishing links between the data and the source media, as well as the data and the crime scene or suspect. The ECtHR practice is centred on trial proceedings and procedural rights, while arguably the development of a principled approach for evaluating the integrity, authenticity, and reliability of digital evidence, particularly in view of the pre-trial investigation phase, could be a pre-condition to maintain the effectiveness of this evidence rule in the digital domain. This case law being comparatively old and predating digital evidence means that, while some conclusions about its applicability to digital forensics investigations may be made by analogy, the established require-

[118] Shulepova v. Russia, no. 34449/03, 11 December 2008, § 62; Poletan and Azirovik v. the former Yugoslav Republic of Macedonia, nos. 26711/07, 32786/10 and 34278/10, 12 May 2016, § 94.
[119] Khodorkovskiy and Lebedev v. Russia, nos. 11082/06 and 13772/05, 25 July 2013, §§ 718 and 721; Poletan and Azirovik v. the former Yugoslav Republic of Macedonia, § 95.
[120] Stoimenov v. the former Yugoslav Republic of Macedonia, no. 17995/02, 5 April 2007, § 38; Matytsina v. Russia, no. 58428/10, 27 March 2014, § 169.
[121] Mantovanelli v. France, no. 21497/93, 18 March 1997, § 33 and 34; Feldbrugge v. the Netherlands, no. 8562/79, 25 May 1986.
[122] Kostovski v. the Netherlands, no. 11454/85, 20 November 1989, § 40.
[123] Feldbrugge v. the Netherlands, cited above; Letinčić v. Croatia, no. 7183/11, 3 May 2016, § 50.
[124] Nideröst-Huber v. Switzerland, no. 18990/91, 18 February 1997, § 24; Lobo Machado v. Portugal, no. 15764/89, 20 February 1996, § 31; Vermeulen v. Belgium, no. 19075/91, 20 February 1996§ 33.
[125] Constantinides v. Greece, no. 76438/12, 6 October 2016, §§ 37-52.
[126] Ibid., Brandstetter v. Austria § 46.
[127] H. v. France, no. 10073/82, 24 October 1989, §§ 61 and 70.
[128] Devinar v. Slovenia, no. 28621/15, 22 May 2018, §§ 48, 51 and 56-58.
[129] Mantovanelli v. France, §§ 33- 34.
[130] Bönisch v. Austria, § 32.
[131] Sakit Zahidov v. Azerbaijan, no. 51164/07, 12 November 2015, §§ 52 –53.
[132] Zahidov v. Azerbaijan, § 56.
[133] Evidence dynamics is typical for the digital data phenomenon defined as "any influence that changes, relocates, obscures, or obliterates evidence regardless of intent" in W. Jerry Chisum and Brent E. Turvey, 'Evidence Dynamics: Locard's Exchange Principle & Crime Reconstruction', (2000) 1 Journal of Behavioral Profiling <http://www.profiling.org/journal/vol1_no1/jbp_ed_january2000_1-1.html>..
[134] P.G. and J.H v. the UK, cited above, § 74.
[135] Gary Edmond and Andrew Roberts, 'Procedural Fairness, the Criminal Trial and Forensic Science and Medicine' (2011) 33 Forensic Science and Medicine 36.

ments for this evidence rule are arguably insufficient to scrutinize digital expert evidence.

5.4.2. *Challenges to technology-assisted expert evidence*

A first set of challenges arise from the fact that all the parties in criminal proceedings demonstrate unscrutinised reliance on research and technology for delivering criminal justice. Digital forensics tools are readily employed while the scientific validity of the experimental and technically complex digital forensic methodology is assumed, so that challenging it on reasonable grounds requires a level of technical literacy. In addition, there is a missing legal framework to ensure that unreliable, exaggerated, or misleading digital evidence will be scrutinized sufficiently for legal decision making.[136] By contrast to fingerprint or DNA analysis where forensics science is used for a task with a limited scope, when digital forensics are applied throughout the whole investigation, the defence opportunity to challenge all the processing stages on valid grounds, to confront the digital forensics examiner, and to have an explanation of the methods and tools is limited. A high financial and time-consuming burden for the defence can be finding digital forensics experts, tools, and preparing accuracy and reliability claims. Digital forensic reports and objective measurements for accessing data integrity, methods and tool reliability validation, and attribution to individuals are not sufficiently produced by the prosecution, which means that digital evidence processing might not be sufficiently documented for further examination by other parties to the proceedings. There is also not a clear standard for digital forensic expert reports, and what the required elements are of such a report in order to evaluate the reliability of the results, e.g., how the system works is often not included in the report, possible errors or alternative interpretations are not mentioned, and the report is focused on reporting results, where the essential data processing steps are not mentioned or chained in an auditable manner. As *Jakobs and Sprangers* argue, forensic experts also have a "natural resistance to publishing information about current investigation methods, in case criminals benefit from that public knowledge."[137] However, this could lead to a parallel construction of evidence and could greatly disadvantage the judicial process.

A second group of challenges arises from the fact that digital forensics method and tool reliability cannot and must not be assumed. Digital forensics emerged from computer engineering which resulted in the lack of a theoretical framework, an underlying scientific methodology and an experimental basis, while peer-review methods, tools, and their validation have short lifespans and rapidly become obsolete. Research into digital forensics and legal regulations for digital evidence and investigative measures are also developed in parallel to address new challenges in technology. The small guild of digital forensic examiners means that the defence might not be able to find a forensic specialist to challenge the evidence where certain methods are not in the competence of a single expert and might require multi-disciplinary validation.

A third challenge is related to the way digital forensic methods and technology are used and implemented by law enforcement. The utility of digital forensics science in respect to all aspects of the investigation leads to the emergence of an investigative and digital forensic science in practice. Because of the investigative expertise needed in addition to the scientific methodology, digital forensics also involves a great deal of subjectivity embedded in the methods and tools used. Digital forensics tools encompass streamlined forensic methodology in a fixed setup to assist law enforcement agents with no or limited digital forensic science knowledge. As important as it is to enable them to perform digital investigation tasks, it also turns LEAs into amateur scientists. This software remains the silent witness which no one challenges, or only a few do. Consequently, the fact that forensics and investigative actions are performed as one makes the quality evaluation of both harder, poses questions about professional bias, protection of innocent defendants and equality of arms in respect to digital forensics aid for the defence .

5.5. *Legal assistance in crucial stages of the evidence handling*

The principle of equality of arms and Art.6 (3) (c) ECHR codify the right to access to a lawyer throughout all criminal proceedings as a fundamental safeguard for fairness. This principle can be transposed as an evidence rule for legal assistance in the crucial stages of evidence handling.

5.5.1. *Case law analysis*

Legal assistance in the crucial stages for the defence stages of the investigation is developed as a safeguard against coercion, ill-treatment, and miscarriage of justice, preventing police misconduct, ensuring respect for the right of an accused not to incriminate him/herself and to remain silent.[138] The court states that the manner in which the right to legal aid is to be applied in pre-trial proceedings depends on the special features of the proceedings involved and on the circumstances of the case. In certain cases, the court has established the essential role of the defence lawyer to test and participate in evidence discovery on pre-trial – namely identification procedures or reconstruction of events and on-site inspections,[139] search and seizure operations,[140] when the accused is taken in

[136] Hans Henseler and Sophie van Loenhout, 'Educating Judges, Prosecutors and Lawyers in the Use of Digital Forensic Experts', (2018) 24 Digital Investigation S76; Joëlle Vuille, 'Admissibility and Appraisal of Scientific Evidence in Continental European Criminal Justice Systems: Past, Present and Future', (2013) 45 Australian Journal of Forensic Sciences 389; Christopher V Marsico, 'CERIAS Tech Report: Computer Evidence v. Daubert: The Coming Conflict', (Purdue University School of Technology, 2004) <https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2005-17.pdf>.

[137] Livia EMP Jakobs and Wim JJM Sprangers, 'A European View on Forensic Expertise and Counter-Expertise' (2000) 11 Criminal Law Forum 375.

[138] Beuze v. Belgium [GC], no. 71409/10, 9 November 2018, §§ 125-130.

[139] İbrahim Öztürk v. Turkey, no. 16500/04, 17 February 2009, §§ 48-49; Türk v. Turkey, no. 51962/12, 31 March 2015, § 47; Mehmet Duman v. Turkey, no. 38740/09, 23 October 2018, § 41.

[140] Ayetullah Ay v. Turkey nos. 29084/07 and 1191/08, 27 October 2020, §§ 135 and 163.

custody,[141] and in cross-border witness examination.[142] The fairness of the proceedings can be undermined due to refusal or difficulties encountered by a lawyer in seeking access to the criminal case file, at the earliest stages of the criminal proceedings or during the pre-trial investigation.[143] In addition, the applicant or defence counsel must have the possibility to question the witness during the investigative stage[144] or when the testimony needs to be obtained in the absence of the person against whom the statement is to be made on the condition that his lawyer was present during the questioning.[145] Art. 6 (3) (e) the right to interpretation applies also to documentary material and the pre-trial proceedings.[146] Consequently, the Court emphasises that certain stages of the investigation have a determinative effect on the defence opportunity to challenge evidence, and its absence in such procedures cannot be compensated at trial.

5.5.2. *Challenges in the digital domain*

Interesting challenges arise in the digital domain, first with respect to defining the digital investigative stages where the defence should be represented. Data searches, digital event reconstructions, attribution based on data examination and analysis are performed with sophisticated and scientific methods of investigation and the resulting digital evidence might be hard to evaluate if the defence lawyer does not receive sufficient information on the processing stages, the digital forensics actions, and the reliability and error rates of the obtained results. In relation to electronic data disclosure cases,[147] the court established that defining criteria for discovering relevant data and exculpatory evidence is also an essential stage of the investigation, and presumably requires legal representation but it is challenging to establish how to facilitate and when to establish such participation.

The Court expressed the view that pre-trial hearings are an important procedural safeguard which can compensate for the handicaps faced by the defence on account of the absence of such a witness from the trial. This in the digital domain could mean that the defence should be present in the determinative phases of the digital evidence examination which cannot be repeated at trial and will negatively impact defence rights.

Further, if the defence is informed only about discovered relevant data or results, the defence has a limited opportunity to challenge digital evidence which is a result of several processing and pre-processing operations.

Considering a more general rule that suspects, accused, and defendants must have adequate representation and the right to interpretation, it can be questioned if the legal assistance in digital investigation is sufficient. The defence lawyer is ill equipped to perform a digital forensics examination and analysis of data sets and the defence must also not be dependent on digital forensics tools results or the prosecution expert. This leads to the question whether the defence in certain cases should be granted access to digital forensic aid both in relation to expertise and technology.

6. PI-based evidence rules

As the presumption of innocence is a central principle the evidence rules derived from it are examined in greater detail elsewhere,[148] to establish their theoretical foundation and technology-related application in investigations.[148] This section only *briefly* summarises four particularly relevant evidence rules based on the PI and *some* of the identified challenges, at this point to reasonably substantiate the need for addressing these challenges holistically by a reliability validation framework before undertaking the in-depth analysis contextually.

The presumption of innocence encompasses the principles that *(i)* the members of a court should not start with the preconceived idea that the accused has committed the offence charged; *(ii)* the burden of proof is on the prosecution, and *(iii)* any doubt should benefit the accused.[149] Although the ECtHR has stated that in principle the PI does not apply in the absence of a criminal charge against an individual,[150] the principle has always been interpreted to apply to the entire criminal procedure, irrespective of the outcome of the prosecution, and not solely to the examination of the merits of the charge.[151] In recent years, evidence scholars have argued for a broader interpretation of the PI in order to address limitations in contemporary investigations such as its "disciplinary effect in relation to the evaluation of evidence" and "verification of information" from different sources[152]; evidence protection mechanisms[153]; its protection against indication-based data collection practices[154]; and its meaning in technology-facilitated and data-driven investigations.[155] Although the focus here is

[141] Simeonovi v. Bulgaria [GC], cited above, § 111.
[142] A.M. v Italy, no 37019/97, 14 December 1999, §§ 26-27.
[143] Beuze v. Belgium [GC], § 135.
[144] Palchik v. Ukraine, no. 16980/06, 2 March 2017, § 50; Šmajgl v. Slovenia, no. 29187/10, 4 October 2016, § 63.
[145] Šmajgl v. Slovenia, § 63.
[146] Kamasinski v. Austria, no. 9783/82,19 December 1989, § 74; Hermi v. Italy [GC], no. 18114/02, 18 October 2006, § 70; Baytar v. Turkey, no. 45440/04, 14 October 2014, § 49.
[147] Sigurður Einarsson and Others v. Iceland and Rook v. Germany, cited above.
[148] Radina Stoykova, 'The Presumption of Innocence as a Source for Universal Rules on Digital Evidence' (2021) 22 Computer Law Review International 74.
[149] Barberà, Messegué and Jabardo v. Spain, § 77
[150] Gogitidze and Others v. Georgia, no. 36862/05, 12 May 2015, §§ 125-126; Khodorkovskiy and Lebedev v. Russia § 543
[151] Poncelet v. Belgium, 44418/07, 30 March 2010, § 50; Minelli v. Switzerland, no. 8660/79, 25 March 1983, § 30; Garycki v. Poland, no. 14348/02, 6 February 2007, § 68.
[152] Elies Van Sliedregt, 'A contemporary reflection on the presumption of innocence', (2009) Vol. 80 Revue internationale de droit penal 247.
[153] Jackson and Summers (n 25) 199.
[154] Liz Campbell, 'Criminal Labels, the European Convention on Human Rights and the Presumption of Innocence' (2013) 76 The Modern Law Review 681.
[155] 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.

on extending the protection afforded by the PI within the digital forensics domain, those considerations are also reflected.

6.1. *Accurate fact-finding*

The evidence rule of accurate fact-finding is derived from the principle protection function of the presumption of innocence against wrongful conviction, transposing the requirements for a high burden of proof and the obligation of the prosecution to present sufficient evidence therefor.

6.1.1. *Case law analysis*

Even though the burden of proof for the guilt of the suspect lies on the prosecution (and the judge in continental legal systems), this is without prejudice to the obligation to collect both inculpatory and exculpatory evidence. Factual accuracy is not the only objective of criminal proceedings and can be balanced against retributive justice objectives, e.g., evidence obtained through coercion might be excluded even if it is accurate. In addition, the requirement of guilt to be established in accordance with the law does not imply that unlawfully obtained evidence cannot be used, but it requires evaluation as to how the use of the evidence will impact the ability of the defence to present its case.[156] Often the lack of a fair procedure to obtain evidence during an investigation can have a serious impact on this ability and it is not necessarily remedied at trial.[157]

The ECtHR accommodates both the common law standard of proof "beyond reasonable doubt",[158] and the civil law systems' principle *in dubio pro reo*.[159] Art. 6 (2) ECHR, at least with respect to the determination of guilt, requires proof beyond reasonable doubt, and "will prevail over contrary domestic statutory provision of a lower standard".[160] The formulation of the ECtHR, however, is at the level of principle, which creates uncertainties as to the stricter evidential and persuasion burden in common law systems, and some vagueness of terms in respect to digital technologies supporting the generation of evidence. As identified by *Stumer*, continental law systems do not regard the burden of proof as determinative of the risk of non-persuasion, but only of the burden to produce evidence, unlike common law systems where the court may indeed base a conviction on the failure of the defendant to discharge that burden, even if the court is not convinced of guilt beyond reasonable doubt.[161]

Equally notable: neither of these standards of proof require absolute legal certainty. The official interpretation of the presumption of innocence includes the requirement that a verdict should be based on "direct or indirect evidence sufficiently strong in the eyes of the law to establish his guilt."[162]

6.1.2. *Challenges in the digital domain*

In technology-assisted investigations questions arise as to how probability and plausibility of digital forensics findings should be evaluated to comply with the principle of the PI. As digital evidence examination gives only probabilistic outcomes, it needs to be asked:

- What level of accuracy or probability should be achieved in order to conclude that the digital artefacts support guiltiness? or
- What are the criteria for suitable hypotheses and methods to test them in order to comply with the PI?

Another question is whether the technology used in digital forensics can support such a level of testing and accuracy, and overall, what might be the appropriate standard for accuracy in digital forensics. Certain evidence data processing tasks can be fully automated to reduce data volume and complexity, but they might still have a bearing on establishing someone's guilt. This leads to the idea that investigative technology must be designed for the specific purposes of criminal procedures – namely including certain mechanisms that provide protection of innocent suspects, e.g., by technology-design less susceptible to biases by combining various algorithms. Such implementation, however, is, as it would seem, not considered in the currently available all-purpose tools and off-the-shelf algorithms.

Further challenges originating from evidence being digital are:

- how can the integrity of the data set in each individual case be validated by forensic examiners?
- are the digital forensics actions clear and suitable for contesting?
- are both the applied algorithm and the applied feature selection suitable to the particular forensic task? and
- are errors reported, and if so, does that happen in a meaningful way enabling rectification?

– all of which are prone to impact the accuracy of the fact finding and thereby the PI.

A third type of challenge is the lack of statistics or independent research on how digital forensic methods and technologies are adopted and used by LEA.[163] For example, excerpts of content data without the necessary digital forensic examination and analyses, taking into account various factors of the environment and state from which such content data originates, cannot be considered authentic or trustful. *De facto*, however, digital photos, emails, or instant messages are routinely accepted in court as evidence without digital forensics examination, while powerful methods exist to manipu-

[156] Schenk v. Switzerland, no. 10862/84, 12 July 1988, §§ 46-37 and 50-51.
[157] Saunders v. UK, no. 19187/91, 17 December 1996, § 74.
[158] Bykov v. Russia, § 50.
[159] Barberà, Messegué and Jabardo v. Spain, § 77.
[160] Colin Tapper and Rupert Cross, Cross and Tapper on Evidence (12th ed, Oxford University Press 2010) 145–147.
[161] Andrew C Stumer, Presumption of Innocence: Evidential and Human Rights Perspectives (Hart 2010).
[162] Yearbook of the European Convention on Human Rights, 1963, p.740.
[163] Christopher S Koper, Cynthia Lum and James J Willis, 'Optimizing the Use of Technology in Policing: Results and Implications from a Multi-Site Study of the Social, Organizational, and Behavioural Aspects of Implementing Police Technologies' (2014) 8 Policing: A Journal of Policy and Practice 212; Bart Custers and Bas Vergouw, 'Promising Policing Technologies: Experiences, Obstacles and Police Needs Regarding Law Enforcement Technologies' (2015) 31 Computer Law & Security Review 518.

late digital content to such an effect that, at least with regards to imagery, a lot of expertise may be required to uncover such manipulation. If the context of content data is omitted this can distort the evaluation of the digital evidence and the meaning attributed to it, resulting in false assumptions on the degree to which the defendant was involved in the criminal activity and therefore the severity of her/his conviction.

6.2. *Protection against prejudicial effects in the evidence procedure*

The protection against prejudicial effects is an evidence rule that aims at removing biases overtly or covertly inherent to the handling of evidence and affecting a fair and non-prejudiced judgement.

6.2.1. *Case law analysis*

The PI as a rule of treatment requires the court not to start with a preconceived idea of guilt, which is extended to prejudicial statements of state officials at the pre-trial stage[164] or before a formal charge is raised,[165] but also affording protection against statements that prejudge the assessment of the facts by the competent authority,[166] or adverse pretrial publicity by the prosecutor.[167]

While traditionally the protection afforded was aimed rather at prejudicial effects arising from public statements, the very same effects can occur in context of any circumstances that distort the judge's view on and evaluation of the evidence presented in court to the effect that such an evaluation will no longer be neutral but will be impacted by circumstances outside of the criminal procedure and inaccessible to legal evaluation to the disadvantage of the accused. The more sophisticated the evaluation of such evidence is, the more this evidence rule needs to be interpreted in a broader sense. Where the probative value and the accuracy of evidence can only be evaluated by experts, while the common-sense judgement of the judge would be insufficient to draw any meaningful conclusions in that sense, apparently considerations on prejudicial effects need to be extended to the pre-trial analysis of evidence underlying the reports presented as evidence in court.

6.2.2. *Challenges in the digital domain*

Digital investigations are particularly challenging in that respect, given that prejudicial statements can be embedded covertly and subtly in the technology itself, which hides and emphasises their effects on the PI. For example, assumptions of guilt can be set as part of the parameterisation of a tool, by the selection of search method and keywords, or can influence the choice of input or interpretation of the output. In the worst case, this could lead to parallel construction of evidence and reverse burden of proof.

Put in a broader perspective, the rule of treatment can be interpreted as protection against prejudicial effects inherent in the evidence procedure. Prejudicial effects occur when the reliability of the evidence would seem non-proportionate in the light of the potential adverse effects to the individual. In other words, it could be argued that the PI requires an evaluation of the potential reliability and probative value of the evidence against the strength of prejudice caused by the evidence in question.

Although the Court takes the stand that the evaluation of prejudicial evidence effects is reserved to national courts,[168] which leaves this evidence rule somewhat underdeveloped in the ECtHR case law, it can be argued that these novel challenges in the digital domain mandate the Court to develop at least a principle approach to evaluating prejudicial effects rooted in technology.

6.3. *Protection against reverse burden of proof*[169]

In principle, the PI is violated when the burden of proof is shifted from the prosecution to the suspect or defendant.[170] Such a shift, referred to as a reversed burden of proof, where for legal or for factual reasons the defendant finds herself in a position to prove her innocence.

6.3.1. *Case law analysis*

In the *Philips, Murray* and *Telfner* decisions, the ECtHR ruled on the impermissibility of a reversed burden of proof.[171] Likewise, the court has developed its case law on the limitations of such protection. Therefore, certain presumptions of fact and law, or asymmetric rules of proof, though unfavourable for the accused, can be permissible, as long as within the applicable legislation they are confined withing reasonable limits, proportionate to what is at stake and not substantially undermining the rights of the defence.[172] Likewise such presumptions can be acceptable, as the ECthR ruled in *Murray*, a strong *prima facie* case has been established by the prosecution and therefore the evidence does not allow for any other common-sense inference.[173] By contrast, in *Telfner* establishing a presumption where the evidence was weak, was considered re-

[164] Khuzhin and others v. Russia, no. 13470/02, 23 October 2008; Sekanina v. Austria, no. 13126/87, 25 August 1993.
[165] Allenet de Ribemont v. France, no. 15175/89, 07 August 1996.
[166] Ismoilov and Others v. Russia, no. 2947/06, 24 April 2008, § 161; Butkevičius v. Lithuania, no. 48297/99, 26 March 2002, § 53.
[167] Turyev v. Russia, no. 20758/04, 11 October 2016, § 21.
[168] Edwards and Lewis v. the United Kingdom, nos. 39647/98 and 40461/98, 27 October 2004 and Van Mechelen and Others v. the Netherlands, nos. 21363/93, 21364/93, 21427/93 and 22056/93, 23 April 1997.
[169] This sub-paragraph is based on excerpts from the article: Radina Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence' (2021) 42 Computer Law & Security Review 105575.
[170] Telfner v. Austria, no. 33501/96, 20 March 2001, § 15.
[171] Philips v. The United Kingdom, no. 41087/98, 5 July 2001, §32; John Murray v. the United Kingdom [GC], no. 18731/91, 8 February 1996, § 54; and Telfner v. Austria, cited above.
[172] Salabiaku v. France, no. 10519/83, 7 October 1988, § 28: "Article 6 § 2 does not therefore regard presumptions of fact or of law provided for in the criminal law with indifference. It requires States to confine them within reasonable limits which take into account the importance of what is at stake and maintain the rights of the defense".
[173] John Murray v. the UK, cited above, § 52 and §§ 60-62.

versing the burden of proof and therefore a violation of the PI principle.[174]

These judgements show that the Court is attentive to evidence irregularities in the investigation procedure. However, under the fourth instance limitation the court only states that legal presumptions depend on "the importance of what is at stake".[175] It fails to establish to what extent the presumption of innocence could be limited in order to achieve other important goals of the criminal process, and when such limitations amount to a violation. In the digital context, this risks being falsely interpreted as entailing erosion of the PI in the name of effectivity-focused investigative measures. The use of technology allows to obfuscate an intentional or unintentional circumvention of the prohibition of a reversed burden of proof by extensive use of probabilities and assumptions about "digital facts".

Further, in *Marper* the ECtHR dismissed the argument of the prosecution that specific technology and expert knowledge to render certain information intelligible were not at their disposal – and concluded that the abstract possibility is sufficient to be considered an interference with Art.8.[176] Moreover, any data which is irrelevant for the purpose for which it is obtained must be immediately destroyed, storage of evidence data after the trial must be regulated by law and judicial authorisation is considered the main safeguard against arbitrary and abusive surveillance practices.[177] In addition, the Court endorsed the need of secure storage and security clearance for dissemination of intercepted material to be guaranteed.[178] The ECtHR underlined that even "*public information* can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is also where such information concerns a person's distant past."[179] The Court also outlined the particular danger of data collection with "the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes."[180]

6.3.2. *Challenges in the digital domain*

While in exceptional cases a minor limitation to the prohibition of a burden of proof may be acceptable in certain conditions,[181] a report on evidence gathering practices shows that many countries are "lowering the thresholds (reasonable suspicion or serious indications to simple indications, reversed burden of proof, legal presumptions of guilt) for triggering the criminal investigation and for imposing coercive measures, the presumption *innocentiae* is undermined and replaced by objective security measures".[182] Also, *Hamer* argues that when "the cost or probability of wrongful conviction is relatively low, and the cost or probability of mistaken acquittal relatively high, it may be necessary to lower the standard of proof, or even to reverse the burden of proof".

By contrast, *Milaj and Bonnici*[183] examine the use of several technologies to surveil and to collect intelligence on targeted suspects and conclude that these undermine the PI principle and result in a *de facto* reverse burden of proof because of the danger of a parallel construction of facts, collection of extensive personal information which undermines the right to remain silent, circumventing protective mechanisms in the criminal process, and "precooking" evidential material long before any charges are pressed. Some forms of criminal profiling may even result in a *de facto* presumption of guilt.[184] The lack of access to information by the suspect to what is considered relevant in such "data expeditions" might prejudice any further adequate defence and denies any protection to individuals with unconventional behaviour who are not criminals.

Stuckenberg further argues that, in practice, given societal sensitivity and media pressure on the judge, the police and the state prosecution, insubstantial and questionable evidence is used to secure a conviction in an almost hysterical manner (as for example in the context of terrorist activity), or where the defendant is the only person to give evidence, this will result in a *de facto* reverse burden of proof to the disadvantage of the accused.[185] As *Gross* argues the "miscarriage of justice" occurs not at trial, but much earlier in the investigation. Time and social pressure can result in law enforcement striving for conviction and identifying the wrong person as the criminal. The amount of data available makes it easier to "gather enough evidence against this innocent suspect [and] the error will ripen into a criminal charge".[186] The impact of such misidentification is emphasised by tech-assisted investigations, where the line between preventive, security and investigation techniques is blurred.

The need for data retention for investigation purposes is well recognized by law enforcement authorities, but fundamentally questioned and criticised within the data protection community. The controversial nature of 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 emphasised by the CJEU when invalidating the Data Retention Directive.[187] However, the UN report concluded that "national legal obligations and private sector data retention

[174] Telfner v. Austria, no. 33501/96, 20 March 2001, § 15.
[175] Salabiaku v. France, no. 10519/83, 7 October 1988, §§ 28-29.
[176] S. and Marper v. The UK, § 75.
[177] Roman Zakharov v. Russia, no. 47143/06, 4 December 2015, §§ 255-256.
[178] Kennedy v. The United Kingdom, no. 26839/05, 18 May 2010, §§ 162-163.
[179] Rotaru v. Romania, cited above, §§ 43 - 46. Emphasises mine.
[180] S. and Marper v. The UK - in relation to fingerprint.
[181] Trechsel and Summers (n 42) ch 7.
[182] John AE Vervaele, 'Special Procedural Measures and the Protection of Human Rights
 General Report' (2009) 5 Utrecht Law Review 66.
[183] Jonida Milaj and Jeanne Pia Mifsud Bonnici, 'Unwitting Subjects of Surveillance and the Presumption of Innocence' (2014) 30 Computer Law & Security Review 419.
[184] Hildebrandt (n 155).
[185] Carl-Friedrich Stuckenberg, Untersuchungen Zur Unschuldsvermutung: (DE GRUYTER 1998) ch 3 <https://www.degruyter.com/view/books/9783110906349/9783110906349/9783110906349.xml> accessed 15 July 2020.
[186] Samuel Gross, 'The Risks of Death: Why Erroneous Convictions Are Common in Capital Cases (Symposium: The New York Death Penalty in Context)' [1996] Articles <https://repository.law.umich.edu/articles/193>.
[187] Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others [2014] ECLI:EU:C:2014:238.

and disclosure polices vary widely by country, industry and type of data. Some countries report challenges in obtaining data from service providers."[188] In the Tele2Sverige case[189] the CJEU decided that a general obligation for collection of traffic and location data by all service providers for the purpose of combating crime is not in compliance with EU data protection legislation and required the collection to be limited to only what is strictly necessary and proportionate.

The classical portrayal of data retention practices by police as a privacy issue must be enriched by considerations of its impact on the PI. Firstly, there is the need to examine a couple of important safeguards in data retention practices formulated by the ECtHR in relation to Art. 8 ECHR violations but relevant by analogy to the PI discussion. The storage of data has to be subject to strict time limits even when it concerns serious crimes; and individuals must have the opportunity to challenge the retention and the truthfulness of the records.[190] Moreover, the court underlined that the mere storing of data amounts to interference with Art. 8 but failed to clarify the question of "subsequent use of stored data".[191] For example, questionable practices were described as – "function creep" or "surplus information"[192] where digital evidence collected for a certain purpose may end up being used for a different purpose. In Sweden, Finland, and Denmark information collected during wire-tapping or computer surveillance, which exceeds the scope of the investigation, is not regulated by law.[193] This surplus information could be used as evidence in other cases, or likewise serve for investigation and crime prevention purposes. While this may not yet be *per se* an issue in every possible case, the Swedish Council on Legislation (Lagrådet) has rightfully pointed out that specific regulation on the use of surplus information is needed in order to comply with the obligations under Art. 8 ECHR.[194]

Until now, the impact of data retention practices on the PI has not been examined by the Court but by applying by analogy the logic of the case law developed in relation to Art.8, a couple of threats to the PI shall be outlined here. Firstly, data retention as a form of systematic collection of data on individuals risks reversing the burden of proof by confronting individuals with large and comprehensive data sets, inaccuracies of which will be hard to prove for the individual.

Secondly, a lot of the work related to infringements of the PI facilitated by technology is focused on examining cases of high intensity, such as mass surveillance cases or advanced antiterrorist measures. As *de Hert* argues, in the past "enhancing both the reliability and the 'softness' of surveillance measures contributes to their legal receptiveness and apparently silences civil liberty arguments."[195] After examining data retention or the use of biometrics for security purposes as a form of "soft" surveillance, the author outlines the difficulties in applying the principles of proportionality and subsidiarity as legal tests for the intrusiveness of the measure.

In summary, to face criminal threats to society facilitated by technology, states introduce both at the substantive and procedural levels tech-facilitated measures which require balancing the benefits they may have for fighting crime with not only data protection requirements but also the presumption of innocence. In addition to data protection impact assessments therefore, the presumption of innocence must be taken into consideration in further development of robust data retention legislation for law enforcement, specifically focused on the further processing of such data by automated means, the restriction to the use of newly inferred data, and the issue of repurposing and merging of data from different data bases and sources with different levels of accuracy.

This evidence rule which protects suspects and defendants against a reversed burden of proof is in close connection to the proposed reliability standards. Challenges of such "datafication" are related to data collection operations for pro-active evidence collection may result in overreliance on data to identify a suspect *ab initio* and to construct further evidence, especially when using data retention and surplus of information for indication-based analysis and profiling, as well as extensive surveillance in general. Such datafication is likely to create overwhelming datasets of digital evidence, which given limited resources and absence of information on reliability, will be hard to impossible to contest by the defendant at trial. Therefore, in view of these limitations, the mere existence of such datasets, originally collected independently of reasonable suspicion against the accused, is prone to result in a *de facto* reversed burden of proof, if reliability would be taken for granted without reliability validation, and thereby turning the prosecution's burden to prove the accuracy of both the data itself and the inferences made thereof into a defendant's burden to prove their inaccuracy.

7. Amplifying effects: cross-border evidence gathering

Traditionally all the principles that Art 6 ECHR encompasses are being developed for and interpreted in view of a single case, with underlying national criminal proceedings, and therefore predominantly in a trial-centric context. Fair trial principles however are universal and fundamental; and at least in principle, they can guide procedural justice safeguards in a process with multiple jurisdictions and stakeholders driven by the inherent evidence rules.

[188] United Nations Office on Drugs and Crime (UNODC) (n 13).
[189] Joined Cases C-203/15 Tele2 Sverige AB v Postochtelestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others [2016] ECLI:EU:C:2016:970, § 108-109.
[190] S. and Marper v. The United Kingdom, nos. 30562/04 and 30566/04, 4 December 2008; and Rotaru v. Romania [GC], no. 28341/95, 4 May 2000, §§ 43-44.
[191] S. and Marper v. the UK, § 67; and Amann v. Switzerland, § 69.
[192] FP7-SECT-2007-217862, DETECTER project, The use of surplus information in the court of law, 2007.
[193] EU Network of Independent Experts on Fundamental Rights, Opinion on the status of illegally obtained evidence in criminal procedures in the Member States of the European Union, CFR-CDF.opinion3-2003, available at: https://sites.uclouvain.be/cridho/documents/Avis.CFR-CDF/Avis2003/CFR-CDF.opinion3-2003.pdf.
[194] FP7-SECT-2007-217862, Detecter project, The use of surplus information in the court of law, 2007.
[195] Paul JA De Hert, 'Balancing Security and Liberty within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies after 9/11', (2005) 1 Utrecht Law Review 68.

However, their interpretation and implementation in such a context is not well-developed by ECtHR, not least in view of its specific and limited jurisdiction. The available ECtHR case law shall be examined, also because of it serving as an inspiration for legal scholars to examine possible solutions for cross-border investigative cooperation. The analysis is complemented with additional observations on the mutual trust regime in the European Union jurisdiction and its drawbacks in the context of digital investigations, as additional complexity arises from the use of forensic science and technology in cross-border cooperation.

In general, the ECtHR exempts from its jurisdiction matters of admissibility of evidence gathered from abroad and insists that evidence rules are reserved national matters. However, concerning extradition and mutual legal assistance,[196] where one state is party to ECHR and the other is not, the Court has examined the responsibility of states that are Party to the ECHR under Art. 6 ECHR, thereby establishing case law on the extra-territorial effects of the provision. Two distinct approaches in the Court's reasoning can be identified.

Firstly, already in older case law the Court recognized that even when Art. 6 ECHR is not directly applicable in extra-territorial cross-border cases it has a reduced, indirect effect considering flagrant denial of justice.

Soering was an extradition case where the ECtHR for the first time recognized an extradition decision being part of the criminal procedure and that therefore a contracting party to the Convention must consider in such decisions any serious, concrete, and severe consequences for the defendant in the receiving country,[197] stating that an issue might *exceptionally be raised* under Art. 6 ECHR in circumstances where the fugitive has suffered or risks suffering *a flagrant denial of a fair trial in the requesting country*[198] "as to amount to a nullification, or destruction of *the very essence*" of Art. 6.[199] Conversely, in *Drozd*, where Andorra as a non-contracting party to the ECHR failed to ensure a fair trial, raising questions on the lawfulness of the subsequent detention in France under Art.5 ECHR, the Court found that the formal administrative and judicial review of the extradition was sufficient without further examination of Art. 6 ECHR violations in non-contracting countries.

Secondly, however, in the evaluation of mutual legal assistance procedures for *evidence gathering* the Court's reasoning is different. In the case of *Pellegrini*, where the annulment of a marriage by the Vatican Court was deemed enforceable by the Italian courts, the Court departed from the flagrant denial of justice doctrine and examined Art. 6 ECHR violations in full, stating that this was of *capital importance* for the parties.[200]

In cross-border evidence gathering the ECtHR seeks a balance of the individual interests against the public interest of effective cross-border cooperation in criminal investigations, where crucial stages of the procedure must be evaluated from the defence standpoint. As argued by *Wijk* in such cases the ECtHR performs a full evaluation of Art. 6 ECHR requirements and considers the cross-border cooperation as an extension of the criminal procedure in the requesting state.[201] However, many issues related to cross-border transfer of unlawfully obtained or unreliable evidence concern the admissibility of such evidence in the receiving country. Given the limited jurisdiction of the ECtHR where questions of admissibility remain under sole jurisdiction of the national court, such cases may remain at a national level, and may not be examined against the requirements of Art. 6 ECHR. Consequently, the ECtHR examines formal procedural requirements for compliance, but does not develop a principled approach for the evaluation of foreign evidence evaluation in terms of evidence law in cross-border scenarios.

This is of particular relevance for digital evidence, as by its nature it can be copied and easily exchanged, and may serve in hundreds of cases across many jurisdictions. Simultaneously the defendant's difficulties in contesting the lawfulness and reliability of such digital evidence unequally increase, as the process of obtaining and analysing such evidence across different countries may remain obscure, and the exact circumstances of obtaining and analysing that evidence might not even be known to the prosecution receiving and using it, be it due to confidentiality requirements in the country of origin or lack of investigating these circumstances. This results in the lack of an effective remedy for the defence to scrutinize foreign evidence – its origin, reliability, and lawfulness, and lack of a procedural framework for judicial evaluation.

ECtHR case law addressing these issues is therefore relatively sparse. In the case of *A.M v. Italy*,[202] where the Italian prosecutor refused the accused and his lawyer participation in the examination of US-based witnesses, the ECtHR found a violation of Art. 6 (3) (d) ECHR, in that particular case the conviction being based solely and decisively on the statements of these witnesses. In *Echeverri Rodriguez v. the Netherlands* the Court stated that the use of evidence of foreign origin in domestic procedures can invoke state responsibility under ECHR, while emphasizing that effective scrutiny of such evidence during the trial, and not during investigation, was the most important safeguard. That approach may fail for the previously mentioned reasons of a potential lack of relevant information on the lawful obtaining and reliable processing of the evidence, not least in the light of the princi-

[196] For a comprehensive analysis of see: Trechsel, S Gless, 'Transnational Cooperation in Criminal Matters and the Guarantee of a Fair Trial', AAH van Hoek and MJJP Luchtman, 'Transnational cooperation in criminal matters and the safeguarding of human rights'; Vogler, Richard (2013) Transnational inquiries and the protection of human rights in the case-law of the European Court of Human Rights. In: Ruggeri, Stefano (ed.) Transnational inquiries and the protection of fundamental rights in criminal proceedings: a study in memory of Vittorio Grevi and Giovanni Tranchina. Springer, Heidelberg, pp. 27-40. ISBN 9783642320118; Wijk (p.20 and following).

[197] Soering v UK, Judgement of 7 July 1989, §§ 85-88.

[198] Soering v UK, Judgement of 7 July 1989, § 113. Emphasis mine.

[199] Al Nashiri v. Romania, App. No. 33234/12, § 717 (May 31, 2018); and Othman (Abu Qatada) v. United Kingdom, App. No. 8139/09, § 260 (May 9, 2012)

[200] Pellegrini v. Italy, no. 30882/96, Court (second section), Judgment (Merits and just satisfaction) 10 July 2001, § 40.

[201] Marloes C van Wijk, Cross-border evidence gathering: equality of arms within the EU?, Eleven International Publishing, 2017, 21–24.

[202] ibid., A.M. v Italy, §§ 26-27.

ple of non-enquiry not allowing one country to scrutinize another jurisdiction's measures. Additionally, the Court required such claims to be substantiated by the defence, which appears surprising in view of the burden of proof principle. Such a requirement substantially disadvantaging the defence has been criticised,[203] and it would also appear to be inconsistent with the previously analysed ECtHR case law in non-cross-border cases, where the ECtHR underlined the importance of examining the pre-trial proceedings in order to ensure a fair trial.

The more recent case of *Stojkovic*[204] is an example of more rigorous examination of Art. 6 ECHR in respect to evidence obtained during cross-border cases. The Court required the application of the *lex mitior* principle, since the defence lawyer was not present in the questioning of the French suspect in Belgium, while under French law this guarantee is required. The Court held that the French investigating judge failed to ensure the higher procedural guarantee for the accused according to French law, and therefore did not comply with Art. 6 ECHR. The Court insisted on efficient defence rights protection in the investigative stages which are crucial for the defence. However, this case does not include a digital evidence gathering procedure. As argued further the forensic examination of digital evidence is also a crucial stage of the investigation which requires effective remedies for the defence. Sometimes the digital forensic process might be split between the cooperating states. In such cases, identifying the origin, chain of custody, and validating the procedure of cross-border digital evidence exchange is crucial for the judicial process in the requesting state.

In summary, the Court importantly extends the Art. 6 ECHR to reach to cross-border cooperation in criminal proceedings and account for the need to balance the individual interests against the public interest in cross-border cooperation, even in cases where this results in an extra-territorial effect. However, in the examination of the responsibility of the executing state for their investigative action and the responsibility of the requesting state for the use of foreign evidence at trial, the ECtHR seems to fall back behind its own case-law in domestic cases, when limiting evidence scrutiny to the trial and excluding the investigation phase in cross-border cases. Likewise, requiring the defendant to substantiate potential issues with the lawfulness of obtaining the evidence in the country of origin or the reliability of such evidence, especially in the digital domain where such substantiation is hardly possible with reasonable effort for the defendant, would appear to come close to a reverse burden of proof.

7.1. *Presumption within presumption: mutual trust and human rights in EU law?*

After the *Lisbon Treaty*, the ECHR, the European charter of fundamental rights (CFR)[205] and the national constitutional traditions are all sources of human rights law in the European Union legal order. Currently, CFR plays a decisive role to guarantee an effective judicial protection in the implementation and interpretation of the multilevel human rights law in the EU. Its horizontal effect must accommodate discrepancies between EU primary law, EU secondary law and national implementations or interpretations by ensuring effective access to the courts.

The *Lisbon treaty* includes important changes with regard to criminal procedure based on Art. 67 TFEU in conjunction with Art. 82(1) TFEU, which requires the creation of an area of freedom, security and justice (AFSJ) in Europe. The creation of the AFSJ includes approximation of substantive criminal laws for serious crimes including computer crime and approximation of criminal procedure, developing investigation information exchange policies and mutual admissibility of evidence, as well as minimum rules on the right of individuals and victims in criminal proceedings.[206]

The mutual recognition principle is based on the presumption that all countries respect the fundamental rights and have sufficient safeguards for them in their criminal procedures. This construct is a bit shaky because one presumption (compliance with mutual trust requirements) lays over another presumption (respect for human rights). Both presumptions aim to work also in the very dynamic and sensitive environment of digital evidence and investigations. It is interesting that exactly the adverse effect on the autonomy and effectiveness of the mutual trust principle in EU law became a major argument for CJEU to reject the draft agreement for the accession of the EU to the ECHR.[207]

This regime is specifically designed to enable law enforcement cooperation in criminal investigations by ensuring full compliance with ECHR by all parties. The ECtHR established the *Bosphorus presumption* according to which the ECtHR will presume that states actions under the EU jurisdiction are in accordance with the ECHR as long as EU law "is considered to protect fundamental rights (…) in a manner which can be considered at least equivalent to that for which the Convention provides".[208] Therefore, it is further examined whether the mutual trust regime delivers better answers to the identified Art. 6 gaps in the ECtHR case law and if it provides guidance on common evidence law in cross-border investigations.

[203] Wijk (n 201); Sabine Gless, 'Transnational Access to Evidence, Witnesses, and Suspects' in Darryl K Brown, Jenia Iontcheva Turner and Bettina Weisser (eds), Sabine Gless, The Oxford Handbook of Criminal Process (Oxford University Press 2019) <http://oxfordhandbooks.com/view/10.1093/oxfordhb/9780190659837.001.0001/oxfordhb-9780190659837-e-33> accessed 1 December 2020; Aukje AH Van Hoek and Michiel JJP Luchtman, 'Transnational Cooperation in Criminal Matters and the Safeguarding of Human Rights' (2005) 1 Utrecht Law Review 1; Richard Vogler, A World View of Criminal Justice (Ashgate 2005).

[204] Stojkovic v France and Belgium, Judgment of the Court of 27 October 2011, § 41.

[205] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

[206] Roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings, adopted pursuant to the Stockholm Programme <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1462894&t=f&l=en> accessed 12.12.2021.

[207] CJEU, Opinion 02/2013 Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms — Compatibility of the draft agreement with the EU and FEU Treaties.

[208] Bosphorus Airlines v Ireland, appl. no. 45036/98, § 155.

In *Melloni*,[209] the CJEU had to decide if the right to a fair trial, as codified in the Spanish Constitution, can impose limitations on provisions of the Arrest Warrant Directive.[210] CJEU states that according to Art.53 CFR the protection of human rights is guaranteed by each respective jurisdiction in the EU according to *their respective fields of application*. This means that mutual trust investigative instruments are exclusively under EU jurisdiction, and member states have no jurisdiction to impose their codification of human rights, even if they have higher standards than the ECHR minimum guarantees. In *Opinion 2/13* the Court stated that member states cannot require a "higher level of national protection of fundamental rights" in the EU legal system, and such a system might require that the country does not check whether other member states have actually, in a specific case, observed the fundamental rights.[211] Apart from clarifying that the evaluation of the fair trial protection in the context of mutual trust falls exclusively under EU law and CJEU jurisdiction,[212] the Court left the impression that the human rights level of protection depends on the particular security goal EU law tries to achieve, and this often could be on the preference for security. Consequently, while in *Stojkovic* the ECtHR requires when one of the cooperating parties has a higher procedural protection for the defence to be preferred, the CJEU openly states that mutual trust interests might prevail against higher human rights protection.

Several scholars commented in respect of the *Melloni* and *Radu*[213] judgements, that the CJEU focus on effectiveness of mutual recognition instruments must not be such as to turn the ECHR minimum human rights standards into the maximum in EU security policy.[214] Moreover, in its Green Paper of 2003[215] the EU Commission referred to the importance of "the right to have evidence handled fairly" in cross-border investigation. Six years later another objective was pointed out in an EU Commission statement when referring to the collection of evidence in cross-border cases when stating that there is a need of "minimum principles to facilitate the mutual admissibility of evidence between Member States, *including scientific evidence*."[216] A core safeguard is that "the treatment of suspects and the rights of the defence would not only not suffer from the implementation of the principle [of mutual recognition] but that the safeguards would *even be improved through the process*".[217]

7.2. *Reconciling the fair trial principle with the mutual trust principle*

Several arguments can be made that the EU legislator currently does not succeed in reconciling the human rights objectives with the mutual trust principle. Each of those arguments is exemplified briefly bellow, since a full analysis of the topic goes beyond the purposes of this paper.

- EU legislation enacted in the ASFJ is focused on trial guarantees and traditional fair trial rights but does not interpret them in the new context of EU cross border cooperation and does not clarify the principles application in the investigative stage of the proceedings.

It is notable that in the whole *Roadmap for strengthening the procedural rights of suspected or accused persons in criminal proceedings*, adopted pursuant to the Stockholm Programme,[218] the focus is set on classical rights like the right to interpretation and a lawyer, which are all guaranteed by the ECHR. For example, the Directive 2016/343 was adopted and entered into force in 2018 to strengthen the presumption of innocence principle in EU. The Directive does not explicitly state where it codifies higher standards than the ECHR and this will open the door to interpretation issues. Further, there are no provisions on suspects' rights regarding the collection and exchange of digital evidence or on the prosecutors' obligation to collect exculpatory evidence. Art. 6 ECHR explicitly states that the burden of proof is on the prosecution and any doubt should be to the benefit of the defendant. The provisions follow the ECtHR jurisprudence that presumptions of fact and of law are not contrary to PI as long as they are under strict limits. Moreover, Recital 22 goes a step further by clarifying that "reasonable limits" require such presumptions to respect the rights of the defendant, to be "proportionate to the legitimate aim pursued" and rebuttable, which give the opportunity for the defence to challenge the prosecution and provide exculpatory evidence. However, the EU Commission's proposal of Article 5 (2) which required the justification of reverse burden and explicitly stated that defence evidence which raises reasonable doubt is sufficient for rebuttal,[219] became a point of

[209] C-399/11 Stefano Melloni v Ministerio Fiscal (GC) ECLI:EU:C:2013:107.
[210] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision [2002] OJ L190/1.
[211] Ibid., Opinion 02/2013, § 192.
[212] For a comprehensive analysis see Justin Lindeboom, 'Why EU Law Claims Supremacy' (2018) 38 Oxford Journal of Legal Studies 328.
[213] C-396/11 Ciprian Vasile Radu (GC) [2013] ECLI:EU:C:2013:39.
[214] Paul de Hert, 'EU Criminal Law and Fundamental Rights' in Valsamis Mitsilegas and Maria Bergstrom (eds), Research handbook on EU criminal law (Edward Elgar Publishing 2016) 113.- referring to Anagnostopoulos and the German national court.
[215] EU Commission, Green Paper Procedural Safeguards for Suspects and Defendants in Criminal Proceedings throughout the European Union /* COM/2003/0075 final, 2.6.
[216] EU Commission, Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility, COM/2009/0624 final. Emphasises mine.
[217] European Commission, Green Paper - Procedural Safeguards for Suspects and Defendants in Criminal Proceedings throughout the European Union /* COM/2003/0075 final */. Emphasis mine.
[218] Legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings 2013/0409(COD) - 26/10/2016 <https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1462894&t=f&l=en> accessed 12.12.2021.
[219] European Commission's Proposal for a Directive 2016/343/EU of the European Parliament and the Council on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings <http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290821_/com_com%282013%290821_en.pdf> accessed 12.12.2021.

disagreement in the adoption negotiations and the final text is an unsatisfactory political compromise, which according to the EU Commission could hamper "legal certainty, control and operability".[220]

A study of the main differences among countries impacted negatively by the EU criminal law development stated that "[e]xclusionary rules developed in the Access to a Lawyer and Presumption of Innocence Directives were scrapped in the final text, thus undermining their added-value to the current framework of evidence law."[221] For example, Art.4 in conjunction with Recital 16 was interpreted by CJEU as not regulating pre-trial detention decisions.[222] By contrast, the *Advocate General* underlines the direct link between the right to liberty and the presumption of innocence,[223] the tension between the two in the evidence evaluation and in the reasoning of the detention decision,[224] and derives PI-based substantive rules on evidence. Reading Art. 6 ECHR and Art. 48 CFR in conjunction with Art.3 and Art.4 of Directive 2016/343/EU, even if *prima facie* evaluation of evidence for detention does not directly infringe the PI, it might be insufficient to meet the "reasonable suspicion" criterion.[225] Moreover, when the decision for detention is disputed, not taking into consideration and comparing both the incriminating and the exculpatory evidence, even if the reasonable suspicion criterion is met, may in fact infringe the PI.

Arguably, the AG, although only in relation to judicial decisions on pre-trial, derived a direct evidence rule from the PI. Although not endorsed by the CJEU, the *Advocate General* opinion is an example of the importance of the right to a fair trial and the inherent PI standards as a harmonization tool for evidence rules at the investigative stage. However, the CJEU only underlines that the overlap between Art. 6 ECHR, Art.48 CFR and Art.4 of the Directive requires as a safeguard the justification of the detention decision in the form of evidence, but ruled that pre-trial detention procedures and evidence rules are reserved for national law and fall outside the scope of the Directive. The Court did not even examine the logical nexus between the PI and the right to an effective defence under Art.48 (2) CFR. It is not surprising, since the CJEU follows the current ECtHR practice of not examining evidence rules and their relation to the PI as an area that remains under national jurisdiction.

It is hard to understand how EU mutual trust investigative measures and mutual admissibility of evidence objectives will be achieved without any harmonization of minimum evidence rules and standards.[226] Further, *Gless* points out that "national criminal procedures lack any special law governing the admissibility of evidence from abroad"[227] She examines the problem with cross-border cooperation in a defendant-centric approach. As will be shown in the *Encrochat* digital investigation, digital evidence is deepening the divide not only between the defence and prosecution, but also between the prosecution and the trial judge. Apart from the burden of proof provision, the Directive does not address any issues on admissibility, reliability, or illegality of obtained evidence.

- EIO and newly proposed mutual recognition-based instruments do not contain efficient safeguards for a fair trial in digital evidence processing or with respect to novel forensic science evidence and technology and does not address issues of defence evidence gathering sufficiently.

EIO is a judicial decision, which has been issued or validated by a judicial authority of a member state, to have one or more specific investigative measure(s) carried out in another member state to obtain evidence. In addition, EIO may be requested by a suspected or accused person.[228] It is a single instrument in a standardized form, providing time limits (30 days for recognition and another 90 for execution) and limited grounds for refusal with respect to human rights and data protection (e.g., a. proportionality and necessity test in the issuing state and the right of the executing state to opt for a less intrusive measure). Art. 6 EIO Directive requires firstly that the issuing state performs a necessity and proportionality assessment of the investigative measure *taking into account the rights of the suspected or accused person*. Secondly, the requested investigative measure must be available in similar domestic cases. As argued by *Armada* there is "no common threshold in the EIO for resorting to coercive investigative techniques. The necessity and proportionality conditions consequently leave a wide margin of discretion to the issuing authorities".[229] Moreover, the Directive does not include any specific procedure to ensure that the proportionality evaluation is performed or that is based on evidence rules.

The EIO regime does not contain efficient safeguards for evidence processing or with respect to novel forensic science evidence and technology and does not address issues of defence evidence gathering sufficiently. It does not stipulate how the evidence should be collected and preserved or transferred. There are no rules on copies of evidence or retention periods for, and no guarantee for applying certain standards by, the ex-

[220] María Luisa Villamarín López, The presumption of innocence in Directive 2016/343/EU/EU/EU of 9 March 2016, ERA Forum (2017) 18: 335. See footnote 15 referring to the Commission's opinion.
[221] Elodie Sellier and Anne Weyembergh, 'Criminal Procedural Laws across the European Union – A Comparative Analysis of Selected Main Differences and the Impact They Have over the Development of EU Legislation - Think Tank' (2018) <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU%282018%29604977> accessed 17 July 2020.
[222] Case C-310/18 PPU Emil Milev [2018] ECLI:EU:C:2018:732.
[223] Case C–310/18 PPU, Opinion of Advocate General Wathelet, ECLI:EU:C:2018:645, § 62.
[224] Ibid §§ 78-79.
[225] Ibid § 80.
[226] For the discussion on the need for minimum evidence standards see, for example, Martyna Kusak, Mutual Admissibility of Evidence in Criminal Matters in the EU: A Study of Telephone Tapping and House Search (Maklu 2016) 243; Martyna Kusak, 'Mutual Admissibility of Evidence and the European Investigation Order: Aspirations Lost in Reality' (2019) 19 ERA Forum 391.
[227] Gless (n 82).
[228] Ibid., Directive 2014/41/EU, Art. 1 (1) and (3).
[229] Inés Armada, 'The European Investigation Order and the Lack of European Standards for Gathering Evidence: Is a Fundamental Rights-Based Refusal the Solution?' (2015) 6 New Journal of European Criminal Law 8.

ecuting state when gathering the evidence. The Directive does not include any specific rules on how the admissibility and reliability of foreign evidence for such a purpose can be proved and assessed.

According to the *forum regit actum* principle, evidence processing is governed by rules in the requesting state. Art.9 (2) requires the executing state to "comply with the formalities and procedures expressly indicated by the issuing authority" except when they are "contrary to the fundamental principles of law of the executing State". There are several issues examined by scholars in respect of this principle. *Kusak* argues that it is questionable if *forum regit actum* can overcome jurisdictional differences for evidence handling, since *(i)* it does not ensure admissibility of the evidence; *(ii)* it lacks transparent rules in terms of the lawfulness of the way evidence is gathered; *(iii)* and can be applied only in the case of the gathered evidence, meaning that already existing evidence cannot fall within its scope.[230] *Armada* argues that it is questionable if determining the evidence rules in the EIO form is in compliance with the ECtHR requirement for foreseeability of law, which requires to "foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[231] Consequently, the intended empowering of the requested state to secure reliable and admissible evidence is not achieved while the proportionality assessment of the investigation measure in the requesting state is limited. It is also unclear to what extent the proportionality assessment of the investigative measure will ensure fair trial compliance if the evidence processing operations are not governed by such an evaluation and depend on negotiation between states with different evidence laws. Moreover, the ECHR in the case of national responsibility requires clear rules on surveillance and interception such as the state to regulate "the conditions on which public authorities are empowered to resort to any such measures[232] and the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[233] It appears that the EIO regime allows such matters to be negotiated and agreed between the two states, where no provision guarantees the individual's interests and protection.

The control over the intrusive investigative measures by the executing state is also limited. Under Art.11(1)(f) the executing state can refuse the execution of EIO on fundamental rights grounds. This provision refers to the violation of the executing state's obligations and not to the violation of the individual's rights, which some authors interpret as turning the individual into an object of the criminal procedure.[234] However, this approach might be more suitable in an investigation where the evidence gathering concerns large amounts of data and suspects. According to Art. 10 (3) the executing state also has the right to choose less intrusive measures than the those requested. Art. 28 (4) codifies an exception to the *forum regit actum* principle in intrusive procedures concerning evidence gathering in real time, continuously and over a certain period of time. Such operations are governed by the rules of the executing state, which is unclear in relation to para (2) of the same article stating that the operation must be agreed between the two states.

As argued, the position of the defence to collect and contest mutual recognition-assisted evidence processing is very limited. For example, Art 1(3) EIO Directive provides that EIO can be issued based on a defence request. However, the provision makes such assistance *dependent on the national criminal procedure and the assistance of the law enforcement authority.*

Further, in order to enable cross-border evidence exchange in the European Union, the EU commission developed the E-evidence proposals, which aim to facilitate European Production and Preservation orders[235] and in addition entered into negotiations with the USA for an Agreement on cross-border access to electronic evidence.[236] Analysis of these developments is out of scope here, but it should be noted that these legislative initiatives also do not address defence procedural rights, digital forensics questions or evidence reliability standards.[237] As argued by *Tosza* the EIO regime does not "attempt to unify or harmonise the law of evidence", while the proposed European production order lacks "any safeguards for ensuring the accuracy and reliability of digital data for criminal proceedings".[238] The mutual recognition regime lies uneasily with the need for minimum procedural guarantees where "persons concerned are either allowed to claim specific rights that accrue to them in a specific national case, or be allowed to claim the best of both worlds, or should be subject to EU level minimum standards with regard to the execution of investigative measures."[239]

Similarly, the Directives adopted within the EU roadmap for strengthening procedural rights of suspected or accused

[230] Martyna Kusak, 'Mutual Admissibility of Evidence and the European Investigation Order: Aspirations Lost in Reality', (2019) 19 ERA Forum 391.
[231] Armada (n 229).
[232] Roman Zakharov, cited above, § 229; see also Malone, cited above, § 67, Leander, cited above, § 51; Huvig v. France, § 29.
[233] Roman Zakharov, cited above, § 230, Malone, cited above, § 68;
[234] AL Smeulers, 'The Position of the Individual in International Criminal Cooperation' in JAE Vervaele (ed), European evidence warrant. Transnational judicial inquiries in the EU (Intersentia Law Publishers 2005).
[235] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.COM/2018/225 final and additional Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. COM (2018) 226 final.
[236] Information note 7295/21 from the European Commission services following the stock-taking meeting with the US on an EU-US Agreement on cross-border access to electronic evidence, 26 March 2021 (LIMITE).
[237] European Commission, 'E-Evidence - Cross-Border Access to Electronic Evidence' (European Commission - European Commission, 2017) <https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/criminal-justice/e-evidence_en> accessed 18 April 2018.
[238] Stanislaw Tosza, 'All Evidence Is Equal, but Electronic Evidence Is More Equal than Any Other: The Relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law 161.
[239] Vermeulen, De Bondt and Damme (n 12).

persons in criminal proceedings[240] does not contain any regulation on defence evidence gathering or contestability of evidence gathered in cross-border cooperation. Moreover, they do not codify any specific digital forensics rules of procedure or requirements for digital evidence reliability. As *Vermeulen and de Bondt* argue "there is an apparent over-focus on 'traditional fair trial rights,' whereas the most important focus should be on the rights during the pre-trial investigative stage"[241] and more importantly on the effects of mutual-trust based recognition for the protection of fair trial safeguards in a cross-border context. For example, AG *Bobek* stated that "the very core or essence of the right [to a fair trial is] access to the courts."[242] Such overemphasis on the trial stage, examining Art.47 and 48 together, or the scattered case law on PI issues are visible also in the CJEU practice.[243] EU legislators and the CJEU are focused on trial guarantees and standard safeguards already developed in the case law of the ECtHR but fail to examine the new complexities in the context of digital investigations and protecting suspects (defendants) from the improper use of technology.

- The EU Commission and CJEU provided evidence that equal human rights protection in criminal proceedings cannot be presumed.

Consequently, the issue is not the lack of legislation, but the preconceived idea of sufficient implementation and equal standards in the member states and the lack of a clear EU human rights policy. In fact, the EU Commission impact assessment on the PI gave statistics for the opposite[244] – countries understand and apply the PI safeguards in very diverse ways; such differences may have an adverse effect on cross-border application of the principle. Recent alleged rule of law violations in certain member states lead to questioning the impartiality of courts.[245] Apart from the central problem related to the alleged rule of law violations in EU countries and their impact on the EU mutual trust instruments, the *LM decision* exemplifies the lack of a positive human rights policy for criminal procedural cooperation in EU.

8. Conclusion: only partially transposed evidence rules in the digital domain

The provided conceptual framework shows that the right to a fair trial holds abstract principles of fair criminal procedure which can be translated into evidence rules to govern digital evidence at policy level. Those evidence rules substantiate the connection between a fair trial at a principle level, and the evidence law transposing it, without focusing on instrumental, jurisdiction-specific regulations on evidence. However, the exemplified challenges to fair trial and evidence rules in digital investigation suggest a conceptual and practical gap that cannot be fully addressed without rethinking the governance model at large. This mandates an interdisciplinary approach to ensure first and foremost reliability validation.

The ECtHR does not set any requirements regarding the assessment of the reliability of evidence as a matter of national jurisdiction. This is rather disappointing. Firstly, evidence reliability must be guided by a legal theoretical framework which the court can establish without going into matters of admissibility or concrete evidence examination. The ECtHR is well-positioned to establish the requirements and limits of scientific enquiry in criminal matters with respect to the use of intrusive technology for evidence and the fairness of novel digital forensics procedures. Secondly, with guidelines from the ECtHR reliability standards can be harmonized among countries with different legal traditions on the benefit of approximation of procedures, international cooperation, and evidence quality. Thirdly, internationalization and digitalization of criminal evidence requires enforcement of fair trial guarantees much more in relation to procedures, methods, and technology at pre-trial, than classic trial-centric examination. As argued by *Edmond* in respect to digital evidence there are doubts "whether conventional admissibility standards, even in conjunction with trial safeguards, provide jurors and judges with the kinds of information required to rationally assess much of the incriminating expert opinion evidence routinely presented in criminal proceedings."[246]

The analysis showed that the ECtHR endorses the development of a more adversarial and participatory model of investigation procedure. It could be deduced that the ECtHR requires evidence procedures which are consistent across persons and over time and one can comprehend the process and how decisions are made. The ECtHR does not examine jurisdiction-specific admissibility or exclusionary rules but emphasises the need for procedures to ensure contestability of evidence. These arguments endorse a participatory model of evidence procedure where each stake holder has the right to effectively participate in the evidence discourse. The Court endorses the view that representation of the defence is of great importance at certain stages of the investigation which have a determinative effect on the defence opportunity to challenge evidence.

[240] Resolution of the Council of 30 November 2009 on a Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings OJ C 295, 4.12.2009 and the relevant directives <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/rights-suspects-and-accused_en> accessed 12.12.2021.

[241] Wendy De Bondt and Gert Vermeulen, 'The Procedural Rights Debate: A Bridge Too Far or Still Not Far Enough?' (2010) 4 EUCRIM (Freiburg) 163.

[242] Kathleen Gutman, 'The Essence of the Fundamental Right to an Effective Remedy and to a Fair Trial in the Case-Law of the Court of Justice of the European Union: The Best Is Yet to Come?' (2019) 20 German Law Journal 884. - with reference to AG Bobek on p. 889; and

[243] C-399/11 Stefano Melloni v Ministerio Fiscal [2013] EU:C:2013:107; C–396/11 Ciprian Vasile Radu [2013] ECLI:EU:C:2013:39; C-310/18 PPU Emil Milev [2018] ECLI:EU:C:2018:732.

[244] EU Commission, Impact Assessment accompanying the document proposal for measures on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceedings SWD (2013) 478 final, Brussels, 2013, Annex V p.69-70.

[245] C-216/18 PPU Minister for Justice and Equality v LM (GC) [2018] ECLI:EU:C:2018:586.

[246] Gary Edmond, 'Legal versus Non-Legal Approaches to Forensic Science Evidence' (2016) 20 The International Journal of Evidence & Proof 3.

The ECtHR also endorses the importance of judicial oversight early in the investigation with respect to non-disclosed evidence (in order to monitor the relevance to the defence of the withheld information), intrusive investigative measures, witness examination. This shows a tendency towards the comprehensive and principle approach to the investigative stage of the criminal proceedings.

However, this participatory model is not sufficiently developed to address contemporary digital investigations. It has been demonstrated by selected examples that the derived evidence rules face significant challenges in the digital domain. These challenges have a practical impact on the right to a fair trial which cannot be fully addressed by reinterpreting the rule. The first group of equality-of-arms based evidence rules is mostly challenged as the rules needs to be transposed and implemented in the new digital domain. The second group of PI-based evidence rules are challenged rather substantially by technology-assisted investigations which expose missing evidence rules development. One of the preliminary gaps in the case law is the lack of principle approach to reliability evaluation of evidence. The ECtHR sets a strict criterion for the evaluation of questionable evidence related to the quality of the evidence, the opportunity to test its reliability and authenticity and to oppose its use. However, the court does not examine further which procedural guarantees at pre-trial can satisfy these criteria and ensure compliance. The examination of these requirements is mainly in the context of trial proceedings, while arguably the quality and integrity of the investigation procedures must supply most of the information necessary for such an evaluation.

Declaration of Competing Interest

The author declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.