Technical Solutions for Legal Challenges: Equality of Arms in Criminal proceeding

Technical Solutions for Legal Challenges: Equality of Arms in Criminal proceedings.

Serena Quattrocolo[**], Cosimo Anglano[*], Massimo Canonico[*], Marco Guazzone[*]

Abstract. *The paper focuses on how computational models and methods impact on current legal systems, and in particular, on criminal justice. While the discussion about the suitabilty of the exploitation of learning machines and Artificial Intelligence (AI) either as surveillance means and human substitutes in the judicial decision-making process is arising, the authors reflect upon the risk of using AI and algorithm-based evidence in criminal proceedings. The claim of the paper is twofold: on the one hand, we should reinterpret todays legal frameworks, e.g. the European Convention of Human Rights, shifting the attention from possible violations of the right to privacy to potential infringements on a basic fair trial feature, the Equality of Arms. On the other hand, we should aknowledge that main legal issues, triggered by the breathtaking advancements in AI, can properly be addressed mainly through technical solutions (e.g. methods for assessing the completeness and correctness of digital evidence related to mobile devices and conversations). No legal theory, which overlooks the crossover of juridical and computational expertise, will survive the present time.*

Keywords: *Algorithm; Algorithmic Society; Data Protection Law; Evidence; Fair Trial; Technological Convergence; Forensic Analysis; Mobile Forensics; Instant Messaging; Telegram Message.*

1. Introduction

The so-called Fourth Revolution,[1] the digital one, has already transformed and reshaped people's daily lives and their mutual interactions, especially because computational systems are now used as decision tools in many areas of the public and private domain, traditionally ruled by human decisions. Computational modelling, along with artificial intelligence ("AI"), robotics, the internet of things, and more,[2] enacted a trend of delegating decisions to both automated systems and autonomous artificial agents, that has raised a number of critical issues. *Weapons of Math Destruction*, by, Cathy O'Neil, first tried to shake and wake-up the public opinion, with regard to the risks of inequality and discrimination behind the uncontrolled use of big data analytics, able to even **threaten pillars of the rule of law and democracy**.[3] In *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recommendations*, Luciano

[**] Università del Piemonte Orientale, Italy, Law Department. Corresponding author: serena.quattrocolo@uniupo.it This research was financially supported by Università del Piemonte Orientale

[*] Università del Piemonte Orientale, Italy, Computer Science Insitute.

[1] (Floridi 2016).

[2] (Pagallo 2016a).

[3] (O'Neil 2016).

Floridi and his research group, AI4People, extensively focus on the risks of developing a non-properly monitored AI society, setting forth principles and recommendations to be followed either by policy makers and private stakeholders.[4] Thus, we must acknowledge that the use of computational modelling is a matter of normative challenges, both because of possible unfair outcomes - ending up with discrimination – and for the transformative effects it may imply, impinging on autonomy in the decision-making process. Such challenges suggest an overarching concern, triggering issues such as the acceptability of replacing or augmenting human decision-making with algorithms.[5] In particular, after the very famous Compass case,[6] more awareness grew up around the topic of allocating (even partly) judicial decisions to computational models. Being deeply entrenched into the foundational values of the society, criminal justice tends to be considered an 'out-of-reach' realm for technology, whose use in criminal trial is submitted, in many jurisdictions, to the 'Daubert test', stipulated by the U.S. Supreme Court in the Nineties of the past century.[7] However, the proliferation of free-of-cost digital data and of the easily accessible system of processing them is penetrating the domain of criminal justice in various ways.

Within this framework, on December 2018 the CEPEJ[8] released the European Ethical Charter on the Use of AI in Judicial Systems.[9] The soft-law document, based on five principles,[10] sets the spotlight on some general issues that affect any application of computational modelling and artificial intelligence to (continental) judicial systems. Although being not binding, the Charter sets forth minimum standars to start a genuine legally-framed discussion on the topic. In particular, the first principle recommends that the use of AI and other automated justice services is compliant with fundamental rights, being listed by international Covenats and Treaties. In April 2019, the EU Commission

[4] (Floridi et al. 2018). See also (Mittelstadt et al. 2016).

[5] (Pagallo and Durante 2016).

[6] On May 1st, 2017, *The New York Times* reported "the case of Eric L. Loomis, a Wisconsin man, who was sentenced to six years in prison based, in part, on a private company's proprietary software. Mr. Loomis says his right to due process was violated by a judge's consideration of a report generated by the software's secret algorithm, one that Mr. Loomis was unable to inspect or challenge." Adam Liptak, *Sent to Prison by a Software Program's Secret Algorithms*, The New York Times, 1 May 2017, available at https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0 (Last Accessed 7th May 2017).

[7] In the case of Daubert v. Merrel Dow Pharmaceutics, the US Supreme Court (509 U.S. 579 (1993)) intrepreted the Federal Rule of Evidence 702 in the sense that the reliabilty of a scientific theory or method must be evaluated taking into account: a) if the realiability of it has been tested; b) whether it was subject to peer review; c) the known or potential rate of error of it; d) general acceptance of the theory.

[8] The Council of Europe Committee for the Quality of Justice.

[9] Available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c. The Charter sets forth five principles: 1) respect for fundamental rights; 2) non-discrimantion; 3) quality and security; 4)transparency, impartiality and fairness; 5) 'under user's control'.

[10] With many contact-points with the AI4People document (see ftn. 6).

launched its own guidelines for the use of AI, to be monitored over the year, for a possible amendment at the beginning of 2020.

Thus, the aim of the paper is to examine how the use of computational techniques is affecting the current state-of-the-art in some area of criminal law domain, namely evidence. More particularly, focus is, firstly, on the individual right to a fair trial and the Equality of Arms pursuant to Article 6(1) of the European Convention of Human Rights ("ECHR"), coupled with the “minimum rights” to be informed promptly and with adequate time and facilities for the preparation of the defence (Article 6(3) of ECHR). Secondly, and according to the most relevant principles of the European Ethical Charter (in particular, Principle 4), the paper will address some technical solutions to redress the demonstrated shortcomings.

The approach falls within four sets of boundaries. The first is a non-specific use of the terms ‘computational modelling’ and ‘algorithm’. Based on the 2018 Council of Europe study on Algorithms and Human Rights,[11] the sense in which the term algorithm is used in this work refers to Tarleton Gillespie’s 2014 definition of it.[12] The second is that the complexity of digital evidence, in itself, falls out of scope of this paper. A comprehensive literature is growing around the matter of integrating such complexity into the existing framework of the law of evidence: admissibility, reliability, and evaluation of digital evidence make the object of many research projects. A complete review of such literature falls out of our scope. In fact, **the focus of this paper is mainly on the basic *knowledge asymmetry*** that is determined by the recourse to algorithmic systems in the evidence process. The third is the aim to assess how such asymmetry hampers the core of the notion of *fair trial*. In the European context, such concept has been established by the European Convention of Human Rights, drafted by the Council of Europe and signed in Rome in 1950. The European Court of Human Rights case-law then conveyed the notion into the national jurisdictions, reshaping them under several aspects. More recently, the European Union adopted the Charter of the Fundamental Rights, setting forth the principle of fair trail in Art. 47. Thus, this paper focuses on the concept of fair trial as worked out within the system of the European Convention of Human rights.[13] Finally, the fourth boundary is an attempt to assess whether solutions to such asymmetry and to the consequent possible infringement of the fair trail do exist. Approaching the empirical research led by the computer scientists of the team, the paper suggests that the output of such research is an example of suitable instrument to redress the said

[11] See https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

[12] (Gillespie 2014, 167), “Algorithms need not be software: in the broadest sense, they are encoded procedures for transforming input data into a desired output, based on specified calculations. The procedures name both a problem and the steps by which it should be solved. Instructions for navigation may be considered an algorithm, or the mathematical formulas required to predict the movement of a celestial body across the sky”.

[13] According to art. 52 of the Charter of the Fundamental Rights of the EU, to the extent in which the Charter provides for rights and guarantees that are also stated by the ECHR, the meaning and the scope of such rights should be the same. The EU is free to guarantee higher levels of protection.

impairment between the prosecution and the defence, compliant to principle No. 3 of the European Ethical Charter.

The paper, thus, aims to **merge two different methodologies**, that seldom coexist in literature. The legal method, based on documental research and analysis, blends with scientifical empirical research, based on experiments. Therefore, two sets of conclusions are presented in this work. Firstly, the legal documental research demonstrates that the use of algorithm-based evidence and computational modelling in criminal proceedings is likely to impair the equality of arms, infringing the basic feature of the fair trial. Secondly, the experimental research led in forensic analysis, demonstrates that there may be tools to redress such impairment and, thus, to prevent breaches of the fair trial, suggesting that they should be largely applied by prosecution, expert witnesses and courts. Moving from a recent research involving some of the co-authors (that has already been fully published in a scientific journal of the field),[14] the second part of this paper highlights the achievements of that empirical study that are directly related to the matter of validation of automatic-generated evidence.

To this purpose, paragraph 2 addresses the topic of knowledge impairment in criminal proceedings. Paragraph 3 introduces the European Convention's concept of 'equality of arms' and analyses all the risks for fair trial inherent in the use of algorithm-based evidence. Paragraph 4 focuses on a case study, presenting the outputs of the research in forensic analysis, offering validation to information extracted from Telegram instant messaging platform to be used as evidence. Paragraph 5 is devoted to the conclusions.

2. In recent decades, two phenomena have deeply influenced the relationship between law and technology. On the one hand, research into artificial intelligence has resulted in dramatic advances, delivering a scenario in which completely automated processes can mine quintillions of data, progressively gaining knowledge from them, that can be applied in successive mining.[15] On the other hand, the exponential spread of smartphones and other similar internet-based devices has provided easy access to those data, most of which are private conversations, covering sensitive or non-sensitive *personal* data.

As a first consequence of the combination of these two factors, the meaning of private life protection - iconically protected by Art. 8 ECHR[16] - has realigned. First, the traditional places and contexts of such protection (home and correspondence) no longer correspond to the centre of an individual's sphere of privacy. Although 'home' is still the

[14] (Anglano et al. 2017).

[15] See (Pagallo 2017).

[16] Art. 8 ECHR creates a complex system of balances between competing values. The values enshrined in the first paragraph – family life, private life - can be balanced with other issues of general interest, listed thereinafter, under two capital conditions. The first condition is legality; that is to say that such balance must be provided by law. The second condition is that of necessity in a democratic society. For more information see (Quattrocolo, Pagallo 2018, 264 ff.).

preferential site for private life,[17] a substantial part of it is now invested in our electronic devices, which follow our constant movements. As a second consequence, the access to such internet-based devices has become the target of criminal investigations. As a matter of fact, any device, as such, can be a mine of crucial information; moreover, using spyware or malware, for example, to intercept private conversations is a very effective system.[18] By introducing such software onto a smartphone, investigators are able to turn on the device's microphone or camera at any moment, in order to listen to any conversation involving anyone within range of the device, anywhere the person carrying the device goes. Any legal limitation related to place and time of the user's sphere of life is thus ineffective, as the system will intercept everybody (even people getting in contact with the user by chance), at any time and in any place. This scenario makes it quite evident that the pre-existing procedural rules have been almost deprived of effectiveness in this context. However, such activities do not necessarily constitute a breach of Art. 8 par. 1 ECHR especially if such software is considered as just "a different method" for phone-tapping which was consistent with the requirement of "provision by law".

Nevertheless, there is a **clear risk for fundamental rights** inherent in such a scenario. The process of gathering evidence through automated systems brings to the trial process forms of proof whose reliability depends entirely on the accuracy of the digital means being used.[19] Whether a certain conversation occurred in one place or another, at one time or another, to whom an instant messaging account really belongs, are matters of crucial importance in criminal proceedings. How is it possible to assess the correctness of data which was gathered exclusively through an algorithm? Is there any chance to challenge the correctness of such data?[20] **Computational modelling is just the final stage of the long-lasting phenomenon of *knowledge asymmetry***, which is said to have begun when courts started relying on expert evidence in complicated cases.[21]

Principle no. 4 of the European Ethical Charter (*principle of Transparency, Impartiality and Fairness: Make data processing methods accessible and understandable, authorise external audits*) focuses explicitely on this topic. Some have found a solution through access to the digital code regulating the algorithm in accordance with the above-mentioned paradigm of *transparency*[22] (see § 3.1). Unless investigators revert to the specifically crafted systems of accountability,[23] however, such access to the digital code implies that a new algorithm should be at work for almost each subsequent investigation. Whereas this solution can

[17] About "sanctity" of the home, see (De Hert, Gutwirth 2006, 67).

[18] See the study orderd by the Libe Committee of the European Parliament, 'Legal Frameworks for Hacking by Law Enforcement Identification, Evaluation and Comparison of Practices', available at http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

[19] (Van Buskirk, Liu 2006, 20).

[20] (Van Buskirk, Liu 2006, 21).

[21] (Brimicombe-Mungroo 2017).

[22] See, extensively, (Hildebrandt 2013, 239).

[23] See par. 4.2.

be highly ineffective, it nonetheless draws attention to a point that is crucial in this context. Relying on automated systems in order to interfere with an individual's private life for investigative reasons can seriously impair the position of the parties.[24] All in all, substituting traditional technical instruments with completely automated processes brings about two main effects. Firstly, the intrusion is more severe, since the traditional limitations represented by 'home' and 'correspondence' are blurred and accessing a smartphone via malware opens up access to incredible numbers of data.[25] Secondly, the chance to intrude, automatically, into such a broad range of information clearly **impairs the defendant's ability to challenge the evidence,[26] unless they are allowed access to the digital code that is regulating the algorithm.**[27] This new scenario shifts the matter of contention from a problem of interference with private life, to an issue of equality of arms.[28]

3. *Equality of arms*. On the one hand, it is certainly arguable that investigations such as the searches mentioned above through, for example, the use of malware, are fully compliant with the provisions of Art. 8 ECHR. On the other hand, what is evident is that such use implies a huge disproportion between the parties of a criminal proceeding. Whilst prosecutors and police can rely on constantly updated digital resources, the **defendant has almost no opportunity to challenge the 'automated evidence'** against them,[29] unless they are able to access the modelling and logic behind those very resources. We argue that the European Convention can, however, offer a redress for these situations, irrespective of the eventual violation of Art. 8 ECHR. Although the US experience may suggest different conclusions, within the European Convention framwork it really seems that whenever investigations are based on automated access to personal data, the denial of discovery in relation to the digital codes governing the algorithm may amount to a violation of Art. 6 Par. 1 ECHR because it would represent a clear infringement of the principle of equality of arms between the parties.[30]

3.1. This assumption requires some further reflection. First and foremost, it is worth remembering the very essence of the "equality of arms", under the ECHR case-law. As briefly mentioned above, the legal basis for this is Art. 6.1 ECHR, even though no explicit reference to it is provided in the text. Therefore, such a principle has been crafted in the jurisprudence of the Court. At the core of the fairness (consider also the French version

[24] See (Pagallo 2017, par. 3.2).

[25] See, 'Legal Frameworks for Hacking.' See also (Bellovin, Blaze, Clark, Landau, 2014, spec. 22 ff.).

[26] See (Cross 2017).

[27] It is worth reminding the importance, for data accuracy, of the developing researches in the so called *trusted computing*: see (Soni 2017, 35).

[28] "Art. 8 is about substantive issues, Article 6 about procedural rights"; "the transformation of Art. 8 into a source of procedural rights and procedural conditions takes it away from the job it was designed for, [...] to prohibit un reasonable exercises of power and to create zones of opacity" : (De Hert, Gutwirth 2006, 90, 91).

[29] (Vervaele 2014, 124).

[30] (Vervaele 2014, 125, 127).

of the concept, *équité*) of the proceedings, all kinds of proceedings (civil, regulatory, and criminal) have two intertwined features: the adversariness and the equality of arms. Such principles intermingle within the framework of evidence collection and presentation.[31]

Before moving on, it is important to clarify that, within the framework of criminal proceedings, the Court always paid attention to the **natural disparity between the prosecution and the defence**:[32] The public role attached to the first prevents, ideally, any possible identity with the latter. However, this ontological difference between the parties of the criminal proceeding does not affect the capital importance of the principle, inasmuch as it guarantees "each party to be given a reasonable opportunity to present his case under conditions that do not place him at a substantial disadvantage *vis-à-vis* his opponent" (Kress v. France, Gr. Ch., 7.6.2001, par. 72). This is not a declamatory statement, deprived of effectiveness. It implies, as the Court clarified in the very famous case of Brandstetter v. Austria (08/28/1991), that **the parties must be aware of the opponent's statements and allegations and get "a real opportunity to comment" on it** (Par. 67). Thus, "an indirect and purely hypothetical possibility for an accused to comment on prosecution arguments" does not fulfil the Convention requirement, being in breach of the equality of arms. Based on this, the very essence of the guarantee consists of an effective and non-theoretical chance to challenge evidence. We argue that such a chance depends on the inner features of each piece of inculpatory evidence, and when such features rely exclusively on an computational process, the room for effective criticism is hampered.

Although basic within the framework of the fair trial, the right to challenge inculpatory evidence based on unlawful intrusions into private life, is not easy to protect. For example, in the case of Khan vs. UK, 12.5.2000,[33] the Court found a violation of Art. 8 ECHR, because of an unlawful tapping of a private conversation (at the time, the national jurisdiction did not provide for legal regulation of such hidden listening devices), but rejected the alleged violation of art. 6 par. 1, as the applicant was afforded the chance to challenge the authenticity of the recording. In the same way, in the recent case of Svetina v. Slovenia, 22.5.2018, the Court noted that although unlawfully gathered, the evidence obtained by the (illicit) search of the applicant's telephone was not used against him in trial and, in particular, it was not challenged by the latter under the viewpoint of reliability and accuracy (Par. 50). But how could the defendant challenge it?

This leads to the core of our argument: **The reliability of data gathered and processed in an automated manner cannot be challenged in a 'traditional' way**. There is no argument for the defence without having access to some technical information. The main (and apparently impossible) goal is having access to the "hidden algorithm". Therefore, is there an unavoidable violation of Art. 6.1 ECHR, when evidence is collected through algorithms?

[31] See (Chiavario, 2001, 292).

[32] See (Van Dijk, Van Hoof, Van Rijn, Zwack 2018, 563).

[33] See (Jacobs, White, Ovey 2014, 281).

Although equality of arms and fair trial are not absolute human rights, whilst admitting restrictions,[34] the European Court of Human Rights has repeatedly stressed that the ultimate sense of the equality of arms, is a "fair balance" between the parties. This means - to answer the question from which we moved in this paragraph - that the use of automated data, based solely or massively on algorithmic process, without the recourse to any transparency solution, prevents any chance of an effective balance between the parties. Therefore, it potentially implies a breach of Art. 6.1 ECHR.

This conclusion does not push Art. 8 ECHR completely out of the scenario. In some situation, the use of a "non-validated" automated system can also amount to a violation of Art. 8 ECHR. However, this should no longer be a necessary condition for the assessment of the trial's fairness. Such a "shift" would significantly improve the protection of the defendant's rights. A claim of violation of Art. 6.1 should stand on its own, regardless of the eventual unlawfulness of the interference with private life. This would also help in ensuring that the conventional guarantees were constantly updated in relation to the ever-improving technologies that inevitably "filter" into criminal investigations practice, sometimes well below the radar of the existing procedural guarantees.

3.2. Against this scenario, it is worth looking for remedies, if existing. To prevent the risk of infringement of the equality of arms, transparency may be the key to general fairness, and also to trail fairness. The term is used here in a broad sense, to address any possible tool allowing the defence to access, analyse, understand and challenge the algorithm-based piece of evidence.

Transparency can be achieved by demanding the source code (together with inputs and outputs) of the relevant automated process.[35] However, it has been noted that **transparency is not enough, in itself**:[36] Transparency must be meaningful; the disclosure of the source code is not considered true transparency, because only experts can understand it.[37] Moreover, open-source codes may not ensure accountability in all cases.[38] On the one hand, *ex post* verification is often insufficient to validate properties of softwares that were not conceived and designed with accountability in mind.[39] On the other hand, it is often necessary to keep the decision policy at the base of the algorithmic process secret. This is of course the case for software used for investigation purposes, whose effectiveness would be completely hampered with full disclosure.

[34] With specific regard to these issues, (Vervaele 2014, 127).

[35] (Kroll, Huey, Barocas, Felten, Reidenberg, Robinson, Yu, 23).

[36] Transparency does not justify a decision: (Hildebrant 2018, 2 ff.).

[37] (Koene, Webb, Patel 2017, First UnBias Stakeholders workshop, 11).

[38] (Van Buskirk, Liu 2006, 24). (Kroll, Huey, Barocas, Felten, Reidenberg, Robinson, Yu, 23).

[39] (Kroll, Huey, Barocas, Felten, Reidenberg, Robinson, Yu, 24). See also art. 20 of 2016/680 EU directive, implicitly prescribing transparency as a key-feature in designing algorithms and automated systems to mine data in criminal proceedings and investigations.

Are there effective solutions to this scenario? To some extent, one possible solution is referring back to the so called "zero-knowledge proof", that is to say cryptographic tools, allowing to prove that the decision policy that was actually used has certain properties, without disclosing what the decision policy is.[40] Such an instrument seems to allow the defence to challenge accuracy of inculpatory evidence without implying, necessarily, the disclosure of the codes and, therefore, the rewriting of it. However, such a system presupposes that the algorithmic process be designed with this feature from the very beginning. As to the area of the EU, the recent directive 2016/680,[41] on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offence, set some important points.[42] Chapter III deals with the rights of the data subject, this is to say the person whose data is processed. However, even though the text provides for an apparently wide range of access rights, it does not afford the defendant a discovery of the digital codes by the law enforcement agencies,[43] nor does it mention the concept of transparency. Nonetheless, Art. 20 of the directive seems to refer, indirectly, to it, when regulating the stage of designing data-mining software: this would certainly represent an improvement, and reduce shortcomings related to an ex-post impossibility of revising the trustworthiness of the evidence. Moreover, zero-knowledge proof software can help challenge the accuracy of a digital evidence's output, rather than the process of gathering the data. This is to say that it can cast light on the criteria applied to the data mining (of which the digital evidence is the output); such software, however, is not useful in assessing the reliability of data gathered by means of an algorithmic chain (e.g. trojan horses) and used as evidence in trial.

Another possible solution is to ask (and provide) for **independent certification of the algorithms' trustworthiness**, as also recommanded by Principle no. 4 of the European Ethical Charter.[44] An expert-witness could be appointed by the judge to verify the algorithmic process whenever the parties express their doubt about the correctness

[40] (Kroll, Huey, Barocas, Felten, Reidenberg, Robinson, Yu 2017, 30). Authors provide a useful example. Imagine that two millionaires are out to lunch and they agree that the richer of them should pay the bill. However, neither is willing to disclose the amount of her wealth to the other. A zero-knowledge proof allows them both to learn who is wealthier (and thus who should pay the restaurant bill) without revealing how much either is worth.

[41] The directive is part of a two-tier EU initiative, encompassing the regulation 2016/679, about general personal data processing, and the directive itself, regulating, more specifically, data processing for criminal justice purposes. The directive is a more flexible legal instrument, allowing the Member States a certain margin of manoeuvre in its implementation. About the relationship between the two instruments see, (De Hert, Papakstantinou 2016, 9).

[42] However, the directive applies only to data processing that fall within the scope of the EU law.

[43] In fact, it will be up to the MS to strike a proper and effective balance between the two concurrent interests: (De Hert, Papakstantinou 2016, 12).

[44] (Cross 2017b).

of automated data.[45] This would certainly increase the chances to challenge the accuracy, even though it could only be an "indirect" challenge, mediated by the direct experience of the court's expert, whom the defence may not trust. If these seem to be viable solutions to establish a useful standard of transparency in this area, a counterargument can be proposed. It can be said that total transparency could be a double-edged sword, with algorithms being challenged line by line "to the point where the courts no longer function."[46] In fact, introducing a judge-appointed expert-witness would imply, in many of the European jurisdictions, the appointment of parties' own expert-witnesses, with a huge experts' battle about the best way to assess the algorithm accuracy, eventually resulting in the judge's confusion. This is, however, a well-known scenario, that gained momentum with the growing application of science and technology in criminal proceedings. There exists a burgeoning literature on the topic, based on the complicated relations between trials (moving from a fact, backwards to the past) and science (moving from a hypothesis, forward to the future). A fundamental aspect of this relation must be underlined here. Especially in recent decades, criminal justice has witnessed a progressive impairment of the parties caused by the growing recourse to new technologies. **The more evidence becomes technological, the less the parties, and especially the defence, are able to challenge it.** Such impairment has, at least, two reasons. The prosecution is usually able to access to the newest technology, with an "indirect" financial exposure, relying on public money, while the defence seldom can afford it. Moreover, if on the one hand, **the use of automated systems, *per se*, suggests neutrality of the method, discouraging any challenge**,[47] on the other hand, the defence is scarcely afforded the access to the technology that could allow to challenge the prosecutor's methods.

The sense of impairment and inequality between the parties has thus been growing: **when algorithmic accountability is at stake, such impairment seems to overwhelm the whole criminal justice system, representing the breaking point**. And the seriousness of the matter is such that software designers and computer scientists themselves have started researching viable ways to grant the defence convenient certification of accuracy for the algorithm-based evidence brought to trial by prosecutors, as recommanded by Principle no. 3 of the Ethical Charter,[48] providing for quality and security of data.

[45] The directive 2016/680/EU imposes the Data Protection Authorities as independent supervising agencies in the police personal data processing context as well. They may have some role in providing courts with unbiased controls over digital evidence trustworthiness.

[46] (Cross 2017b, 2017a), both quoting Prof. A.J. Brimicombe, Head of the Centre for Geo-Information studies, Univerity of East-London.

[47] (Van Buskirk, Liu, 2006, 21).

[48] 'Principle of Quality and Security: with regard to the processing of judicial decisions and data, use certified sources and intangible data, with models conceived in a mulitdiscipinary manner, in a secure technological environment'.

However, it is crystal-clear, in the Ethical Charter approach, that quality and security of data and modelling necessarily underpin a multi-disciplinary team-work, crossing-over legal and technological expertise to satisfy such a basic principle. Here we present an example of how deeply intermingled the legal and the scientific expertise must be in order to combat serious inequalities.

4. Our case-study focuses on mobile devices, being an integral part of our everyday life, especially by means of suitable applications, installed on our mobile devices. These applications generate, and store on the device, large sets of user data, that may be later used to reconstruct the activities the user carried out. This is true also for criminal activities, whose prosecution is more and more often based on the evidence obtained from the forensic analysis of mobile devices.

Suitable hardware and software tools are typically used by forensic analysts to automate and support the extraction of data from mobile devices, as well as the decoding and correlation of these data with the aim of reconstructing user activities.

While for data extraction these tools follow standardized procedures, that ensure the completeness of the collection, for the decoding and correlation phases the situation is quite different. In particular, while it is true that most prominent mobile forensic platforms[49] are able to decode the data stored by a large number of applications, they do not provide any explanation of how this decoding is performed, nor they provide any guidance on how to correlate different pieces of evidence to completely reconstruct user activities. **Thus, it is impossible to assess the completeness and the correctness of the results generated by them.** Therefore, unfortunately, in most cases the evidence exhibited in the trial is the mere output generated by these tools, with little or no explanation on how the evidence has been obtained from the data stored on the device.[50]

A natural question that thus arises is how to validate the results produced in the trial, without knowing the internals and the workings of the tools used to extract and decode data and of the application. It is evident that such a validation necessarily requires that a complete, correct, and repeatable forensic analysis of the mobile applications used on the device is carried out, in order to compare the results it yields against those produced in the trial.

Such an analysis can be carried out by exploiting a methodology for the forensic analysis of Android applications,[51] presented in a recent research,[52] that is able to ensure the completeness, correctness, and repeatability of the analysis.

Thanks to the use of this methodology, it is possible to fully reconstruct all the user activities by (a) identifying all the artifacts that carry relevant investigative information,

[49] (Cellebrite LTD. 2015b); (Micro Systemation 2016); (Oxygen Forensics, Inc. 2013a); (Compelson Labs 2017).

[50] In violation of both Principle no. 3 and 4 of the European Ethical Charter.

[51] Note that Android is used on nearly 90% of the smartphones sold worldwide, so focusing on it allows to maximize the applicability of this methodology.

[52] (Anglano et al. 2017).

(b) describing how they can be decoded in order to extract that information, and (c) showing how they can be correlated in order to infer information of potential investigative interest that cannot be obtained by considering individual artifacts in isolation. Based on the exploitation of virtualized smartphones in place of physical ones, this methodology is able to achieve very high levels of generality and of reproducibility of the results, having established their accuracy by comparing them with those obtained by using a physical smartphone. Consequently, this methodology has the potential to be used to validate (or refute) the findings presented by a digital forensics expert in a trial, thus preventing infringements of the fair trial.

Altough the complete report of the research has been published in a specialized journal, it is important to refer here to the main achievements of such work, in order to consider whether this kind of methodology can play a valuable role in preventing infringements of the fair trial, according to the goals set forth by the brand new European Ethical Charter.

To illustrate how this can be achieved in practice, in this paper we first describe the above methodology, and then we show how it has been applied to perform a thorough and reproducible analysis of Telegram Messenger, a very popular instant messaging platform [53] that is reportedly used for various criminal activities, ranging from cybercrime[54] to those engaged by various terrorist organizations.[55] The results of this analysis can be used to validate the findings reported by the forensic experts in a trial where the evidence collected from the artifacts generated by Telegram Messenger is exploited. Hence, by confirming or refuting these results, the above methodology can play a valuable role in preventing infringements of the fair trial.

4.1. The methodology under consideration is based on the controlled execution of a set of experiments, using one or more Android devices, and on the inspection and analysis of the internal memory (both persistent and volatile) of these devices. Given that the goal of any forensic analysis is to allow the analyst to obtain the digital evidence generated by the application under consideration, the methodology used to carry it out must exhibit the following properties: 1) completeness: the identification of all the data generated by the application under analysis. To obtain completeness, suitable experiments stressing all the relevant functionalities of the application need to be carried out; 2) repeatability: the possibility for a third-party to replicate the experiments under the same operational conditions, and to obtain the same results. To achieve repeatability, it must be possible for a third-party to use the same set of devices, operating systems versions, and forensic acquisition tools to repeat experiments under the same operational conditions; 3) generality: the results hold for many (possibly all) Android smartphones and versions. To achieve generality, the experiments should be repeated on as many smartphones and Android versions as possible.

[53] In Feb. 2016, the Telegram Messenger LLP company reported that there were 100, 000, 000 active users per month, with 350,000 new users signing up per day: see (Telegram Messenger LLP 2016).

[54] (C. Budd 2016).

[55] (J. Warrick 2016).

In the research presented, completeness has been achieved by designing suitable experiments, by executing them in a systematic way, and by resorting to source code analysis (when possible) to gather additional insights into the behavior of the application and/or in the way it encodes the data it stores locally. To achieve generality, virtualized mobile devices were used instead of physical ones, as they make simple and cost-effective running experiments on a variety of different virtual devices, featuring different hardware and software combinations. Repeatability was also achieved thanks to the use of virtualized smartphones, as they allow a third-party to use virtualized devices identical to those used in the experiments, as well as to control their operational conditions, so that the same conditions holding at the moment of the experiments can be replicated on them (see Principle no. 3 of the Ethical Charter).

The methodology is graphically represented in Figure 1, and consists in a set of subsequent steps, as detailed in the following.

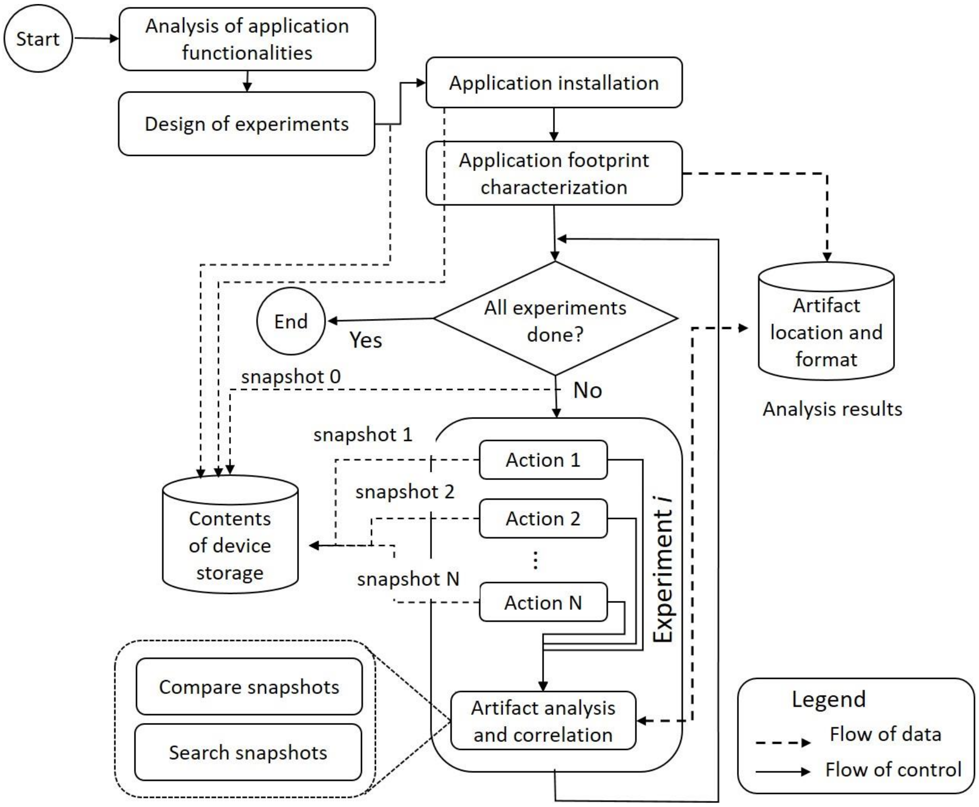

Figure 1The methodology for the forensic analysis of mobile applications.

In the first step, the analyst examines the functionalities of the application, so as to identify those actions that have a potential investigative interest (e.g., sending or receiving a message). Starting from the results of this examination, the analyst designs a set of experiments, in which the above actions will be carried out on the device, in order to elicit the generation and memorization of the corresponding data on the local storage of the device.

After this preliminary step has been completed, the experimental activity starts with the installation of the application on the device. Then, the *application footprint* on the device (i.e., the location where the application is installed, as well as the set of files that are created and/or updated during the installation) is characterized by comparing the contents of the device storage against those collected prior to the installation. The location and the format of these artifacts is recorded into the results of the analysis.

Next, the set of experiments is carried out in a systematic way, until all of them have been performed. As shown in the figure, each experiment consists in a set of actions, each one consisting in one or more interactions with the application, that are carried out by the analyst in a pre-defined order.

Before each experiment starts, and after each one of its actions ends, a snapshot of the local device storage is collected and stored for subsequent analysis. After all the actions of a given experiments have been completed, the analyst compares the various snapshots that have been collected, or searches them for known information (e.g., the text of a message that has been sent), in order to identify which files have been created and/or updated as effect of each action, as well as to determine the data that have been written in, or deleted from, the above files. These findings, jointly with the association of each artifact with the (set of) action(s) that generated them, are recorded into the results of the analysis.

4.2. The evidence that can be obtained from the analysis of Telegram Messenger, and that must be validated in order to make sure that the fair trial is not infringed, can be summarized as follows:

1) **User identifier**: in the Telegram system, each user is uniquely associated with a numerical identifier, which is named *Telegram ID* (or *TID* for brevity), as well as with other (optional) information, such as a user name and a profile photo. *The knowledge of these information allows the analyst to attribute to a specific individual the actions carried out with Telegram Messenger.*

2) **List of contacts**: in Telegram, each user is associated with a list of contacts, i.e., other Telegram users with whom (s)he may communicate. For each contact, Telegram Messenger stores his/her TID, phone number, and profile photo. *The evidentiary importance of the information about contacts is clear, as it allows an investigator to determine whom the user was in contact with, and to possibly determine the real identity of each contact* (i.e., by using his/her TID, phone number, and profile photo).

3) **Chronology and content of message exchanges**: Telegram provides its users with the possibility of carrying out one-to-one, one-to-many, and many-to- many communication by using three types of *dialogs* (named *chats*, *channels*, and *groups*, respectively) where users can exchange both textual and non-textual messages. *The ability of reconstructing the chronology and contents of exchanged messages is of obvious investigative importance, as it allows the investigator to determine with whom the user communicated, when these communications occurred, and what it was exchanged. Furthermore, the identification of the properties of each dialog in which the user was involved with* (i.e., its type, its creator, its date of creation, its administrators, etc.) *may provide valuable evidence in various investigative scenarios*. For instance, the choice of using a secret chat (a form of chat where messages are encrypted end-to-end and they self-destroy after a user-defined amount of time) instead of a regular one may indicate the intention of the users to totally hide the fact they

are communicating. Analogously, the creation and administration of a private (i.e., that cannot be found by the search function of the Telegram platform) group or channel on which illegal material is shared, or unlawful communications are broadcast, may provide evidence that the user was involved in criminal activities (e.g., terrorist propaganda or diffusion of child pornography material).

4) **Chronology of voice calls**: Telegram provides its users with voice calls that, as secret chats, relies on one-to-one communication channels and end-to-end encryption. *The ability of reconstructing the chronology of voice calls (i.e., when a call has been performed, with whom, and for how long) is of evident investigative value*.

The above information will be typically used in court as evidence against the defendant, or, as a means to challenge the accuracy of a chronology or the content of a conversation, or the attribution of these actions to him/her, in case such reconstructive method has not been used. As a matter of fact, the reports generated by state-of-the-art mobile forensic analysis platforms – that are typically used *verbatim* in the trial – do not explain how the above information has been obtained from the data stored in the device (i.e., the location, format, and decoding procedure of these data). Therefore, as already mentioned, it is impossible to challenge the results generated by these platforms, given that their internal workings are unknown.

However, the methodology described before can be used to trace down and validate the results reported by any mobile forensic platform, as it allows to correctly characterize Telegram Messenger in terms of the data it generates and stores on a mobile device, of the location and format of these data, and of the association of user actions with them.

In particular, as reported in the aforementioned paper[56], the application of the forensic analysis methodology to Telegram Messenger has produced the following results: a) all the forensically-relevant artifacts stored by Telegram Messenger on Android smartphones have been identified; b) the structure and format of these artifacts has been determined, so that its correct decoding procedure has been devised; c) the data stored by Telegram Messenger have been mapped to the user actions that generated it; d) using the above mapping, it has been shown how to recover the account used with Telegram Messenger, and **how to reliabily identify the Telegram user who carried out the activity using the device under examination, and to correctly reconstruct (I) the contact list of the user, (II) the chronology and contents of both textual and non-textual messages, and (III) the log of the voice calls done or received by the user**.

By using these results, a defendant may be able to either validate or refute the completeness and the correctness of the reconstructions of his/her actions carried out by means of Telegram Messenger, in case they are used to support allegations against him/her.

[56] (Anglano et al. 2017).

5. The methodology briefly reported here is an important example of how independent review of data generated by automated process may grant validation of evidence. As a matter of fact, once the results of this research have circulated, the level of transparency in using Telegram data and conversations in criminal proceedings will improve in many different ways. Firstly, Law Enforcement Agencies and their experts should, since now on, refer to this wide range of information when searching somebody's mobile phone (or other Internet devices): on the basis of the abovementioned findings, account, user's data, date, duration of a conversation or of other exchanges and many other information should be correctly detected, with a lower risk of miscarriages of justice. Secondly, in case the information is not immediately dealt with in respect of these protocols, the defendant has a wide range of chances, from asking the judge to appoint an expert to validate it, to appointing a defence's experts to confront the conclusions driven by the prosecutor from non-validated data.

Thus, against the arguments that were reported in § 3, it is possible to argue that when transparency is not sufficient, per se, to ensure comprehension of automatic-generated data, an independent review by a judge-appointed expert may redress the risk of a massive disproportion between prosecution and defence in the evidence process. However, this is not always true. The case-study that has been presented here focuses on algorithms and models that were freely accessible to the researchers who experimented the new method. When the access to models is prevented, for the reasons mentioned above - such as matters of intellectual property or secrecy - *ex post* validation and, thus, challenging the accuracy of evidence in court is still prevented.

However, the path has been traced down by the European Ethical Charter for the use of AI in justice systems. Actually, the most clear prescription deriving from that text is the need for a more frequent and fruitful cooperation between lawyers and computer scientists: this will the best tool to preserve the principle of equality of arms in the 21st century.

List of references.

- 504ENSICS Labs, 2016. Linux Memory Extractor (Lime). Available at: http://codeload.github.com/504ensicsLabs/LiME/zip/master.
- Al Barghuthi, N., Said, H., Nov. 2013. Social networks IM forensics: encryption analysis. J. Commun. 8 (11), 708e715.
- Anglano, C., Canonico, M., Guazzone, M., 2017. Configuration and Use of Android Virtual Devices for the Forensic Analysis of Android Applications. Technical Report TR-INF-2017-06-02-UNIPMN.

University of Piemonte Orientale. http://www.di.unipmn.it/TechnicalReports/TR-INF-2017-06-02-UNIPMN.pdf.

- Anglano, C., Canonico, M., Guazzone, M., Dec. 2016. Forensic analysis of the Chat-Secure instant messaging application on Android smartphones. Digit. Investig. 19, 44e59.
- Anglano, C., Sept. 2014. Forensic analysis of WhatsApp messenger on Android smartphones. Digit. Investig. 11 (3), 201e213.
- Archard A. (2006), The Value of Privacy, in Claes, Duff, Gutwirth (eds), *Privacy and the Criminal Law*, Intersentia, 13-31
- Azfar, A., Choo, R., Liu, L., Sept. (2016). An Android communication app forensic taxonomy. J. Forensic Sci. 61 (5).
- Balkin, J. M. (2016) The Three Laws of Robotics in the Age of Big Data, October, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890965 (last accessed 4 February 2017);
- Brimicombe, Allan J., Mungroo, P. (2017), Algorithms in the Dock: Should Machine Learning Be Used in British Courts?, presentation at the 4th Winchester Conference on Trust, Risk, Information and the Law, 3 May 2017.
- Bellovin S.M, Blaze M., Clark S., Landau S. (2014), Lawful Hacking: Using existing vulnerabilities for wiretapping on the Internet, in NW. J. Tech. & Intell. Prop., vol. 12, 1-35.
- Budd, C., Aug. 2016. Following the Mark: Hackers Begin to Leverage Telegram Messaging App. Available at: https://goo.gl/Q84fJe. Cath Corinne, Wachter, Sandra, Mittelstadt, Brent, Taddeo, Mariarosaria and Luciano Floridi (2016)Artificial Intelligence and the 'Good Society': the US, EU, and UK Approach, December, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2906249 (last accessed 4 February 2017);
- Cellebrite LTD, 2015a. UFED Mobile Forensics Applications. Available at: http://www.cellebrite.com/Mobile-Forensics/Applications.
- Cellebrite LTD, 2015b. UFED4PC: the Software-based Mobile Forensics Solution. Available at: http://www.cellebrite.com/Mobile-Forensics/Products/ufed-4pc.
- Chiavario M., (2002) Art. 6, in S. Bartole, B. Conforti, G. Raimondi, Commentario alla convenzione europea dei diritti dell'uomo e delle libertà fondamentali, Padova, 154-248.
- Claes, E., Duff, A., Gutwirth, S. (eds), (2006), Privacy and the Criminal Law, Intersentia,
- Cocq, C., Galli, F. (2013), The catalysing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes, in New Journal of European Criminal Law, Vol. 4 issue 3, 256-289.
- Compelson Labs, 2017. Mobiledit Forensic Express. Available at: http://www.mobiledit.com/forensic-solutions/.
- Cross, M. (2017a), *Justice by algorithms could "bring Courts to an Halt", The Law Society Gazette,* 3.5.2017
- Cross, M. (2017b) ,Algorithms and Schrödringer's Justice, in *The Law Society Gazette*, 8.5.2017
- De Beer D., De Hert P., Gonzalez Fuster G., Gutwirth S. (2010), *Nouveaux eclairages de la Notion de donné personnelle et application audacieuse du critère de proportionalité*, Revue Trimestrielle des Droits de l'Homme, 141-162
- De Hert P. Gutwirth S., (2006) *Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power*, in Cleas, Duff, Gutwirth (eds), *Privacy and the Criminal Law*, Intersentia, 61-104.
- De Hert P., Papakstantinou V. (2016), The New Police and Criminal Justice data protection directive, New Journal of European Criminal Law, Volume 7, Issue 1, 7-19.
- De Schutter P., (2001), *La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme,* Revue Universelle des Droits de l'Homme,
- DrKLO, 2017. Telegram Messenger for Android. Available at: https://github.com/DrKLO/Telegram.
- Epifani, M., Stirparo, P., 2015. Learning iOS Forensics. Packt Publishing.

- Floridi, L. (2012) Big Data and their Epistemological Challenge, *Philosophy & Technology*, 25(4): 435-437
- Google, (2016a). Android Device Monitor. Available at: https://developer.android.com/studio/profile/monitor.html.
- Google, (2016b). Run Apps on the Android Emulator. Available at: https://developer.android.com/studio/run/emulator.html.
- Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Luetge C., Madelin R., Pagallo U., Rossi F., Schafer B., Valke P., Vayena E. (2018), AI4Pople – An Ethical Framework for a Good AI Society: Opportunities, Risks, Pinciples, and Recommendations. Mind and Machines 28, 689-707.
- Goss, R. (2014), *Criminal Fair Trail Rights*, Hart Publishing
- Gregorio, J., Gardel, A., Alarcos, B., (Sept. 2017). Forensic analysis of telegram messenger for windows phone. Digit. Investig. 22, 88e106.
- Grindrod P., (2014) *Mathematical Underpinnings of Analytics: Theory and Applications*. Oxford: Oxford University Press;
- Hildebrandt M. (2018), Algorthimc Regulation and the Rule of Law, The Royal Society. Vol 376, Issue 2018, 1-11.
- Hildebrandt M.,(2013), *Profile transparency by design? Re-enabling double contingency*, in Hildebrandt, de Vries, *Privacy, Due Process and the Computational Turn*, Rutledge, 221-246
- Hildebrandt M. (2006), Privacy and Identity, in Claes, Erick, Duff, Antony, Gutwirth, Serge (eds), Privacy and the Criminal Law, Intersentia, 43-58.
- Hildebrandt M., de Vries, K. (2013), *Privacy, Due Process and the Computational Turn*, Rutledge
- Husain, M.I., Sridhar, R., (2010). iForensics: forensic analysis of instant messaging on smart phones. In: Goel, S. (Ed.), Digital Forensics and Cyber Crime. Vol. 31 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg.
- Jacobs F.J., White R., Ovey C. (2014), *The European Convention on Human Rights*, 6th ed. By Rainey, Wicks and Ovey, Oxford University Press
- Jeon, S., Bang, J., Byun, K., Lee, S., (2012). A recovery method of deleted records for SQLite database. Personal Ubiquotous Comput. 16 (6), 707e715.
- Koene A., Webb, H., Patel, M. (2017), First UnBias Stakeholders Workshop, EPRSC funded research, 2016-18.
- Kroll J. A., Huey J., Barocas, S. Felten E.W., Reidenberg J.R., Robinson D.G., Yu H.(2017), *Accountable Algorithms*, University of Pennsylvania Law Review, 633-705.
- Liptak, A. (2017), *Sent to Prison by a Software Program's Secret Algorithms*, The New York Times, 1 May 2017, available at https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top-news&WT.nav=top-news&_r=0 (Last Accessed 7th May 2017).
- McLoughlin M., (2008). The QCOW2 Image Format. Available at: https://people.gnome.org/markmc/qcow-image-format.html. (Accessed 21 June 2017).
- Mehrotra, T., Mehtre, B.M., Dec 2013. Forensic analysis of Wickr application on Android devices. In: 2013 IEEE International Conference on Computational Intelligence and Computing Research, pp. 1e6.
- Micro Systemation, (201)6. XRY. Available at: http://www.msab.com/xry/xry-currentversion.
- Microsoft Corp, (2017). Windows Phone Emulator for Windows Phone 8. https://msdn.microsoft.com/en-us/library/windows/apps/ff402563(v.vs.105).aspx.
- Mittelstadt, Allo, P. Taddeo M., Wachter S. and Floridi L. (2016) *The Ethics of Algorithms: Mapping the Debate*, *Big Data & Society*, July-December, 1-21;

- O'Neil C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Random House: New York;
- Ovens, K.M., Morison, G., (Jun. 2016). Forensic analysis of Kik messenger on iOS devices. In: Digit. Investig. 17.
- Oxygen Forensics, Inc, (2013a). Oxygen Forensics. Available at: http://www.oxygenforensic.com/en/features/analyst.
- Oxygen Forensics, Inc, (2013b). SQLite Viewer. Available at: http://www.oxygenforensic.com/en/features/analyst/data-viewers/sqlite-viewer.
- Pagallo U. (2016) Even Angels Need the Rules: On AI, Roboethics, and the Law. In *ECAI Proceedings*, G.A. Kaminka et al. (eds.), 209-215. IOS Press, Amsterdam.
- Pagallo U. (2017) *Algo-Rhythms and the Beat of the Legal Drum*, in *Philosophy and Technology*, 2017, 31, 1-18.
- Pagallo U., Durante M. (2016) The Philosophy of Law in an Information Society. In The Routledge Handbook of Philosophy of Information, Floridi L. (ed.), 396-407. Oxon & New York: Routledge;
- Santolaya P. (2012), *The right to a private and family life*, in Garcìa Loca, X., Santolaya P., *Europe of Rights: A Compendium on the European Convention of Human Rights,* Martinus Nijhoff Publishers
- Satrya, G.B., Daely, P.T., Nugroho, M.A., (Oct 2016a). Digital forensic analysis of Telegram Messenger on Android devices. In: 2016 International Conference on Information Communication Technology and Systems (ICTS), pp. 1e7.
- Satrya, G.B., Daely, P.T., Shin, S.Y., (July 2016b). Android forensics analysis: private chat on social messenger. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 430e435.
- Sicurella R., Scalia, V. (2013), *Data mining and profiling in the Area of Freedom, Security and Justice*, New Journal of European Criminal Law, Vol. 14, Issue 4, 409-460.
- Soni P. (2017), *Trust me, I am a... Computer*, in *Computers and Law*, 2017, Febr-March, 35-37.
- Susanka, T. (Jan. 2017). Security Analysis of the Telegram IM. Master's thesis. Czech Technical University in Prague, Faculty of Information Technology. https://www.susanka.eu/files/master-thesis-final.pdf.
- Tamma, R., Tindall, D. (2015). Learning Android Forensics. Packt Publishing.
- Telegram Messenger LLP, (Feb. 2016). 100,000,000 Monthly Active Users. Available at: https://telegram.org/blog/100-million.
- Telegram Messenger LLP, (May 2017a). Binary Data Serialization. Available at: https://core.telegram.org/mtproto/serialize.
- Telegram Messenger LLP, (May 2017b). TL Language. Available at: https://core.telegram.org/mtproto/TL.
- Telegram Messenger LLP, (May 2017c). TL Schema. Available at: https://core.telegram.org/schema.
- Telegram Messengers LLP, 2017. Telegram Applications. Available at: https://telegram.org/apps.
- The Statistics Portal, Oct. 2018. Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2018. https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/
- The Telegram Team, (Jan. 2017). Android Developers Never Sleep. Available at: https://telegram.org/blog/unsend-and-usage#android-developers-never-sleep.
- Tso, Y.-C., Wang, S.-J., Huang, C.-T., Wang, W.-J. (2012). iPhone social networking for evidence investigations using iTunes forensics. In: Proc. of the 6th International Conference on Ubiquitous Information Management and Communication. ICUIMC'12. ACM, New York, NY, USA, pp. 1e7.
- United Nations Office on Drugs and Crime (Feb. 2013). Comprehensive Study on Cybercrime. Tech. rep., United Nations.
- Van Buskirk E., Liu T.V. (2006), Digital Evidence: Challengiong the Presumption of Relability. Journal of Forensic Practice, 19-26.

- Van Dijk P., van Hoof F., van Rijn A., Zwack L. (2018(, Theory and Practice of the European Convention oh Human Rights, Cambridge, Intersentia.

- Verbruggen M. (2006), *The Glass May Be Half-Full or Half-Empty, but It Is Defnitiley Fragile*, in Claes, Duff, Gutwirth (eds), *Privacy and the Criminal Law*, Intersentia, 121-134.

- Vervaele, J.A.E. (2014), Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?, in Gutwirth S., Leenes R., De Hert P., *Reloading Data Protection*, Springer, 114-128.

- Volatility Foundation (2016). An Advanced Memory Forensics Framework. Available at: http://volatilityfoundation.org/.

- Walnycky D., Baggili, I., Marrington, A., Moore, J., Breitinger, F.,(2015). Network and device forensic analysis of Android social-messaging applications. In: Digit. Investig. 14 (Suppl. 1), S77eS84. Proc. of 6th Annual DFRWS Conference.

- Warrick, J., (Dec. 2016). The App of Choice for Jihadists: ISIS Seizes on Internet Tool to Promote Terror. The Washington Post Available at: https://goo.gl/3MKSnP.

- Wu, S., Zhang, Y., Wang, X., Xiong, X., Du, L., (June 2017). Forensic analysis of WeChat on Android smartphones. In: Digit. Investig. 21, 3 e10.

- Zhang, L., Yu, F., Ji, Q., (July 2016). The forensic analysis of WeChat message. In: 2016 Sixth International Conference on Instrumentation Measurement, Computer, Communication and Control (IMCCC), pp. 500e503.

- Zhou, F., Yang, Y., Ding, Z., Sun, G.(June 2015). Dump and analysis of Android volatile memory on Wechat. In: 2015 IEEE International Conference on Communications (ICC), pp. 7151e7156.