Digital Evidence in Human Rights Violations and International Criminal Justice

Tareq Al-Billeh [a,*], Ali Al-Hammouri [a], Tawfiq Khashashneh [b], Mohammad Al Makhmari [c], Hamad Al Kalbani [d]

[a] Faculty of Law, Applied Science Private University, Amman, Jordan.
[b] Faculty of Law, Ajloun National University, Ajloun, Jordan.
[c] Faculty of Law, Sohar University, Sohar, Oman.
[d] Faculty of Law, Arab Open University, Sohar, Oman.

* Corresponding Author: t_billeh@asu.edu.jo

ARTICLE INFO

Article history
Received: August 12, 2024
Revised: December 21, 2024
Accepted: December 22, 2024

Keywords
Digital Evidence;
Human Rights;
International Crimes;
Right to Privacy;

ABSTRACT

The rapid development of the use of digital technologies has facilitated access to digital information and evidence. This information and digital evidence are obtained via the Internet, social media or satellite. And may be used to investigate violations of human rights and international criminal law. Therefore, there is a problem of rebalancing between the right to privacy and the use of information and digital evidence in the investigation of violations of human rights and international criminal law. This study has objective of unified universal principles that set out the origins and rules for the use of information and digital evidence in the investigation of violations of human rights and international criminal law. In order to ensure international and national justice and criminal accountability and to document all violations of human rights and international criminal law. The analytical approach will be used through analysis of previous studies on the use of digital information and evidence in the investigation of violations of human rights and international criminal law. And analysis of the Berkeley Protocol on Open-Source Digital Investigations. Several findings and recommendations were reached in this paper, the most important of which is the need for the international community to recognize the information and digital evidence obtained to demonstrate violations of human rights and international criminal law.

1. Introduction

Digital information and evidence are a complex area at the national and international levels. So, modern technologies that are developing at high-speed complicate issues of monitoring information and digital evidence.[1] In addition, criminals use several modern and advanced tactics to conceal their criminal activities that violate human rights and international criminal law. This makes it more difficult to detect digital information and evidence when committing international crimes. In some practical cases requiring decryption of that evidence,

[1] Jan Gruber, Christopher J. Hargreaves, and Felix C. Freiling, 'Contamination of Digital Evidence: Understanding an Underexposed Risk', *Forensic Science International: Digital Investigation*, 44 (2023), 1-10 https://doi.org/10.1016/j.fsidi.2023.301501

making it more difficult for experts to collect and account for digital information and evidence.[2]

With the continuous technical and technological development of the world's nations, States have the capacity to make extensive use of digital information and evidence. The prosecution of State crimes is one of those areas where information and digital evidence can be used to investigate violations of human rights and international criminal law.[3] It has become possible to rely on evidence and information obtained via the Internet, social media or satellite. Which leads to tracking criminals and suspects, documenting war crimes, crimes against humanity and genocide. So that many data are stored in the digital space, leading to the emergence of new types of criminal offences related to violations of human rights and international criminal law.[4] Therefore, the Internet, social media and satellites are extensively used in the field of surveillance of illegal activities, by providing high-resolution space images of areas experiencing violations of human rights and international criminal law, recording such data and documentation and identifying suspicious activities.[5]

Indeed, the collection of information and digital evidence allows international investigators and international and national jurisdictions to benefit from such evidence and information obtained to detect international crimes. Technological techniques also make it possible to detect illicit operations, monitor the offshore drug and arms trade, and control the movement of ships and aircraft to detect suspicious and illicit movements.[6] Historically, people involved in core activities like smuggling or piracy made up the majority of organised crime's foreign activity. With illicit commodities being exchanged and transported across borders, organised crime has become global, with illicit commodities sourced from one continent, traded across another, and marketed in a third.[7] Thus, as the number, density and complexity of international crimes increase, it is necessary to use

---

[2] Eoghan Casey, Lam Nguyen, Jeffrey Mates, and Scott Lalliss, 'Crowdsourcing Forensics: Creating a Curated Catalog of Digital Forensic Artifacts', *Journal of Forensic Sciences*, 67.5 (2022), 1846–1857 https://doi.org/10.1111/1556-4029.15053

[3] Graeme Horsman, 'Digital Evidence Strategies for Digital Forensic Science Examinations', *Science & Justice*, 63.1 (2023), 116–126 https://doi.org/10.1016/j.scijus.2022.11.004

[4] Tetiana Slipeniuk, Mykola Yankovyi, Viktor Nikitenko, Oleksandr Manzhai, and Yuliia Tiuria, 'Problematic Issues of Using Electronic Evidence in Criminal Proceedings (SDG's)', *Journal of Lifestyle and SDGs Review*, 4.1 (2024), 1-15 https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01867

[5] Mylène Struijk, Spyros Angelopoulos, Carol X.J. Ou, and Robert M. Davison, 'Navigating Digital Transformation through an Information Quality Strategy: Evidence from a Military Organisation', *Information Systems Journal*, 33.4 (2023), 912–952 https://doi.org/10.1111/isj.12430

[6] Office of the United Nations High Commissioner for Human Rights, 'Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal', *Human Rights and Humanitarian Law*, (2022), 1-102 https://doi.org/10.18356/9789210053433

[7] Peter J. Buckley, Peter Enderwick, Linda Hsieh, and Oded Shenkar, 'International business theory and the criminal multinational enterprise', *Journal of World Business*, 59.5 (2024), 1-11 https://doi.org/10.1016/j.jwb.2024.101553

modern and effective means of investigating violations of human rights and international criminal law. Prosecution of war crimes, genocide and crimes against humanity, so that the prosecution of international crimes posed many challenges and material difficulties. So, the use of digital information and evidence would thus detect violations of human rights or contrary to the principles of international criminal law.[8]

The trials based on the principle of universal jurisdiction have steadily increased in recent years. The Rome Statute, which established the integration regime, has undoubtedly had a significant impact on this proliferation.[9] The history of universal jurisdiction can be understood as a rivalry between two ideas relating to the role of a State: the "global executor" approach and the "no safe haven" approach. We could see an example of the "Global Portal" strategy of adopting the Rome Statute at the national level, along with the establishment of war crimes teams throughout Europe. The establishment of war crimes units and the consolidation of basic categories of crimes across different legal systems are important achievements of the integration regime established by the Rome Statute.[10]

The use of open-source digital information and evidence therefore raises a range of questions about the normative framework governing that information and digital evidence before the International Criminal Court. Therefore, the widespread dissemination of such open-source digital information and evidence in the ICC's investigation proceedings has led to the need for such digital information and evidence to be audited by investigators.[11] Such information and digital evidence can have a clear impact on the outcome of the trial, particularly in international cases involving violations of human rights and international criminal law where it is difficult to obtain information and evidence from the traditional crime scene. However, it is noted that open-source digital information and evidence is effectively commensurate with the International Criminal Court's approach to digital information and evidence.[12]

The previous research papers, that find the research paper entitled "'Contamination of Digital Evidence: Understanding an Underexposed Risk". This paper finds that there is a lack of understanding of digital evidence. Multiple

[8] Widya Setiabudi Sumadinata, 'Cybercrime and Global Security Threats: A Challenge In International Law', *Russian Law Journal*, 11.3 (2023), 438-444 https://doi.org/10.52783/rlj.v11i3.1112

[9] Sunardi Sunardi and Ridho Surya Kusuma, 'Digital Evidence Security System Design Using Blockchain Technology', *International Journal of Safety and Security Engineering*, 13.1 (2023), 159–165 https://doi.org/10.18280/ijsse.130118

[10] Karolina Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands', *Journal of International Criminal Justice*, 19.1 (2021), 189–211 https://doi.org/10.1093/jicj/mqab035

[11] Fran Casino, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, and Constantinos Patsakis, 'SoK: Cross-Border Criminal Investigations and Digital Evidence', *Journal of Cybersecurity*, 8.1 (2022), 1-18 https://doi.org/10.1093/cybsec/tyac014

[12] Matthew Gillett, and Wallace Fan, 'Expert Evidence and Digital Open Source Information', *Journal of International Criminal Justice*, 21.4 (2023), 661–693 https://doi.org/10.1093/jicj/mqad050

examples and counter-examples are presented regarding the contamination of digital evidence. As for the research paper entitled "Crowdsourcing Forensics: Creating a Curated Catalog of Digital Forensic Artifacts". This paper finds that the growing amount, diversity, velocity, distribution, structural complexity, and intricacy of digital evidence can hinder practitioners in locating and comprehending the most forensically pertinent material. Digital forensic practitioners presently seek information and answers in a haphazard manner, resulting in outcomes that are unstructured, unverified, and occasionally incomplete. Consequently, some digital evidence is overlooked or misconstrued. To alleviate the dangers associated with knowledge gaps, a systematic mechanism is urgently required for practitioners to codify and integrate their collective knowledge. As for the research paper entitled "Digital Evidence Strategies for Digital Forensic Science Examinations". This paper finds that there is due to the magnitude and complexity of numerous digital forensic device exams, practitioners must systematically and strategically establish a plan of action that enables them to conduct the most thorough and efficient examination feasible. As for the research paper entitled "Problematic Issues of Using Electronic Evidence in Criminal Proceedings (SDG's)". This scholarly article aims to examine the utilization of electronic evidence in criminal procedures, highlighting key problematic aspects, legislative deficiencies, and the necessity for enhancements in law enforcement tactics. By referring to the research paper entitled "Navigating Digital Transformation through an Information Quality Strategy: Evidence from a Military Organisation". This paper finds the utilization of digital technologies for information extraction from diverse data sources can assist Organizations in mitigating uncertainty and enhancing decision-making. The growing volume, pace, and variety of data can pose substantial risks and problems in maintaining a high standard of information quality (IQ).

Through the previous research papers, it becomes clear that our research paper differs from the previous papers through its analysis of the impact of using digital evidence in investigations into violations of human rights and international criminal law, and the extent of the impact of using this digital evidence on the right to privacy. Accordingly, the Berkeley Protocol on Open-Source Digital Investigations establishes several professional standards that must be applied when identifying, collecting, preserving and analyzing open-source digital information and evidence when used in international human rights and criminal investigations and violations.[13]

The paper's importance lies in identifying modern digital methods of investigating and prosecuting violations of human rights and international criminal law. By providing effective tools to international investigators in ensuring that justice is achieved, international criminals are extradited and prosecuted. This

[13] Office of the United Nations High Commissioner for Human Rights, 'Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal', *Human Rights and Humanitarian Law*, (2022), 1-102 https://doi.org/10.18356/9789210053433

is in order to enable the use of digital information in the investigation of violations of human rights and international criminal law to provide geographical information on the whereabouts of international criminals and aerial photography of their whereabouts. And to track international crimes such as war crimes, crimes against humanity, genocide, human trafficking crimes and drug trafficking offences conducted in global geographical spheres by anticipating their future movements. This paper will answer several legal questions, the most important of which are: What digital means can be used to detect international crimes? What are the legal and technical challenges associated with the use of information and digital evidence to prosecute international crimes? How can violations of human rights and international criminal law be monitored through digital evidence and information? Does the use of digital information and evidence to investigate violations of human rights and international criminal law affect the right to privacy.

The research paper aims to study the methods of using digital information to investigate violations of human rights and international criminal law, identify legal and technical aspects associated with the use of digital information, and identify the advantages of the use of digital information and evidence in the detection of international crimes such as genocide, war crimes and crimes against humanity.

2. Research Method

This paper will use the analytical methodology by analyzing previous studies on the use of digital information in investigating violations of human rights and international criminal law, and analyzing the Berkeley Protocol on Open-Source Digital Investigations. We will also refer to studies on digital information and evidence obtained via the Internet, social media or satellite, and the extent to which the use of digital information and evidence in investigating violations of human rights and international criminal law affects the right to privacy.[14] Therefore, the goal of this research study is to conduct a thorough evaluation of the legal framework that governs the information and digital evidence used by the investigating bodies of the International Criminal Court. by drawing attention to the obstacles that the International Criminal Court faces in achieving global criminal justice. Additionally, the International Criminal Court will determine who is qualified to serve as an expert in international criminal investigations. By creating precise guidelines for data and digital evidence in the security information field.[15] This provides particular importance for assessing the impact of such information and evidence obtained and collected from the crime scene. Considering that this information and digital evidence are often obtained and collected remotely by people who have no role in creating it. Thus, there is a need

[14] Dennis G Barten, Derrick Tin, Fredrik Granholm, Diana Rusnak, Frits van Osch, and Gregory Ciottone. 'Attacks on Ukrainian Healthcare Facilities during the First Year of the Full-Scale Russian Invasion of Ukraine', *Conflict and Health*, 17.1 (2023), 1-7 https://doi.org/10.1186/s13031-023-00557-2
[15] Graeme Horsman, 'Digital Evidence and the Crime Scene', *Science & Justice*, 61.6 (2021), 761–770 https://doi.org/10.1016/j.scijus.2021.10.003

to verify that information and digital evidence and to indicate and clarify the technical elements that demonstrate the commission of international crimes. Therefore, the use of specific and consistent standards on digital information and evidence helps experts to control digital information and evidence and to ensure that the procedural rules for collecting digital information and evidence are not violated.[16]

It should be noted that the study of how experts' digital information and evidence is presented has an important role for many organizations seeking to apply international criminal law. Information and digital evidence obtained by experts are used by many international organizations such as UN fact-finding missions whose own reports will be referred to in this paper. Human rights organizations and the International Criminal Court, as well as domestic courts in many cases of heinous crimes under universal jurisdiction. Thus, establishing clear bases for the collection of experts' information and digital evidence is important and necessary to support international criminal justice efforts.[17] Analysis of personal data for information and digital evidence may lead to a violation of the right to privacy, which is a fundamental human right and is enshrined in many international human rights treaties and conventions. In addition, to most of the world's constitutions, technological development has made it easier to collect personal data. Which raised several concerns about the misuse of such personal data in the digital age.[18] Based on the foregoing, the methodology of the study focuses on the use of modern technologies in the collection of information and digital evidence, such as: satellite images analysis. And on the establishment of international crimes committed in difficult-to-reach geographical areas and the prosecution and referral of perpetrators to international courts.

3. Results and Discussion

The Meaning of Digital Information and Evidence

Digital technology has permeated every part of our lives in the modern world. As a result, digital information and evidence are becoming increasingly important in the area of criminal justice. From mobile phones to computer networks, human digital fingerprints can be critical in the investigation and prosecution of international criminal cases. Digital information and evidence support the preservation of just and fair trial, as well as assistance in documenting events and

[16] Ken MacLean, 'Interactive Digital Platforms, Human Rights Fact Production, and the International Criminal Court', *Journal of Human Rights Practice*, 15.1 (2023), 84–99 https://doi.org/10.1093/jhuman/huac062

[17] Özgür Heval Çınar, 'The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age', *The International Journal of Human Rights*, 25.1 (2021), 26-51 https://doi.org/10.1080/13642987.2020.1747443

[18] Muhammad Akhlaq, Hafiz Adil Jahangir, and Hamzullah Khan, 'Defending the Right to Privacy in the Digital Age', *Journal of Policy Research*, 8.4 (2022), 534–538 https://doi.org/10.61506/02.00006

establishing facts that may not be available or invisible to traditional investigative techniques.[19]

Overall, there has been global recognition that digital information and evidence has become more complex as a result of the complex and increasingly sophisticated technology landscape among consumers and companies. Therefore, the impact of cloud computing and the growing proliferation of the Internet of Things pose ongoing challenges for digital forensic analysts and their business. What is most surprising about events is the recognition by many authors of the influence of human factors and the susceptibility of human error in the field of information and digital evidence.[20] Digital forensics is essential for law enforcement in current criminal investigations as technology evolve into tools for unlawful activity and evasion of discovery. A chain of custody is required for successful criminal prosecution in court to ensure the integrity and authenticity of the evidence. However, because digital evidence is delicate and variable, managing its preservation and collecting is a significant difficulty.[21] Therefore, digital evidence and information is meant as data stored or digitally transmitted such as photos, graphic recordings, social media posts, as well as email.[22]

Open-source digital information and evidence means information that is digitally accessible to the public and obtained from the Internet. This includes the data generated by users, and the data developed by the machines. For example, digital information and evidence include: documents, photos, videos and audio recordings found on websites, information-sharing platforms, satellite images and data disseminated by Governments, as well as content posted on social media sites.[23] Thus, digital information and evidence are necessary to investigate violations of human rights and international criminal law. But the use of such digital information and evidence leads to many challenges, such as persistent and rapid changes in technology, and the privacy of digital information and evidence in the international criminal justice system. Those challenges could affect the

[19] Ivan Prysiazhniuk, 'Use of digital evidence in criminal process: some issues of right to privacy protection', *Visegrad Journal on Human Rights*, 5 (2023), 81-88 https://doi.org/10.61345/1339-7915.2023.5.11

[20] Paul Reedy, 'Digital Evidence Review 2016–2019', *Forensic Science International: Synergy*, 2 (2020) 489–520 https://doi.org/10.1016/j.fsisyn.2020.01.015

[21] Fu-Ching Tsai, 'The Application of Blockchain of Custody in Criminal Investigation Process', *Procedia Computer Science*, 192 (2021), 2779-2788 https://doi.org/10.1016/j.procs.2021.09.048

[22] Cameron Brown, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology*, 9.91 (2015), 55–119 https://doi.org/10.5281/zenodo.22387

[23] Office of the United Nations High Commissioner for Human Rights, 'Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal', Human Rights and Humanitarian Law, (2022), 1-102 https://doi.org/10.18356/9789210053433

acceptance and validity of digital information and evidence in international criminal trials.[24]

In fact, digital information and evidence are fragile and volatile, so that they can be modified, erased or easily altered, either deliberately, or after being collected, preserved, handled and stored incorrectly from the outset. Therefore, to preserve this evidence and information, it must be handed over to digital forensics experts in order to avoid its corruption and ensure its integrity, and the integrity of the data and information it carries.[25]

Therefore, the integrity of information and digital evidence stored on technical media is verified by courts in various countries of the world. At the same time, criminal legislation in most of the world's countries does not contain a clear definition of digital information and evidence. This leads to ambiguity in the use of such information and digital evidence when assessed and used in the investigation of violations of human rights and international criminal law. This requires clarification of judicial practices when assessing the acceptance and appropriateness of digital information and evidence during criminal trials for violations of human rights and international criminal law.[26] Documents can be digital or printed documents, including a variety of categories, including official documents, such as military documents, official meeting records, financial records, such as banking transactions, maps and medical records. Some documents may be protected by the right to protect State secrets or privacy rights. Protection must therefore take place in accordance with the State's legal framework and the potential risks of receiving and possessing documents.[27]

In the meantime, experts lack consensus on the understanding, characteristics and role of digital information and evidence within evidentiary sources in international criminal trials. It is proposed that the word "electronic (digital) evidence" should be incorporated into the legislation. This is supported by the fact that the term "electronic" defines the category of device used to create and store evidence, while "digital" relates to the method of recording information on the

[24] Christa Miller, 'A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point', *Forensic Science International: Synergy*. 6 (2023), 1-22 https://doi.org/10.1016/j.fsisyn.2022.100296

[25] Nicholas Akosu, and Ali Selamat, 'Incorporating Language Identification in Digital Forensics Investigation Framework', *Studies in Computational Intelligence*, 555 (2014), 63–78 https://doi.org/10.1007/978-3-319-05885-6_4

[26] Mykhaylo Gutsalyuk, and P. ANTONIUK, 'Procedural Capacity of Use Electronic (Digital) Information as Evidence in Criminal Proceedings', *INFORMATION AND LAW*, 2.41 (2022), 116–22 https://doi.org/10.37750/2616-6798.2022.2(41).270373

[27] Muhammad Akhlaq, Hafiz Adil Jahangir, and Hamzullah Khan, 'Defending the Right to Privacy in the Digital Age', *Journal of Policy Research*, 8.4 (2022), 534–538 https://doi.org/10.61506/02.00006

specific device.[28] In addition, many States such as France, Germany, the Netherlands and Sweden have incorporated provisions into their domestic legislation to enable the exercise of universal jurisdiction as outlined in the Rome Statute. Conversely, states often initiate investigations due to national security concerns arising from the presence of foreign fighters returning to their territories. This illustrates the "no safe haven" policy.[29]

Any investigation into the collection of information and digital evidence must be in line with jurisdictional digital data preservation and disposal policies. And it should be in line with the State's data and digital information governance requirements. Other factors to be taken into account include the impact of digital evidence preservation requirements for litigation, judicial orders for the production and disposal of digital data and information. As well as, challenges associated with the preservation and disposal of digital information and evidence, and costs associated with storage and the disposal of such digital evidence.[30]

The use of digital information and evidence is investigated according to several international processes and standards. First: the acquisition of digital information and evidence, so that a copy of digital data is generated from a particular data source and is an important step in the digital investigation. Because it enables additional examination of digital information and evidence while reducing the risk of digital data loss and manipulation.[31] Second: Examining digital information and evidence by converting digital data into an appropriate form that can be read by the average human being and regulate data around it, and identify potential digital information and evidence.[32] Third: Analyzing digital information and evidence so that the analysis of digital information and evidence is linked to the identification and evaluation of potential sources of digital evidence as information. Evidence and data stored or transmitted in bilateral form and identified through the process of analysis of digital information and evidence as relevant to the investigation.[33] Fourth: Preparing reports on digital information

[28] Tatiana Fomina, and Oleksii Rachinskyi, 'Electronic Evidence in Criminal Proceedings: Problematic Issues of Theory and Practice', *Bulletin of Kharkiv National University of Internal Affairs*, 102.3 (2023), 207–220 https://doi.org/10.32631/v.2023.3.43

[29] Karolina Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands', *Journal of International Criminal Justice*, 19.1 (2021), 189–211 https://doi.org/10.1093/jicj/mqab035

[30] Sarah Zarmsky, 'Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law', *Journal of International Criminal Justice*, 19.1 (2021), 213–225 https://doi.org/10.1093/jicj/mqab048

[31] Animesh Kumar Agrawal, Aman Sharma, Sumitra Ranjan Sinha, and Pallavi Khatri, 'Forensic of an Unrooted Mobile Device', *International Journal of Electronic Security and Digital Forensics*, 12.1 (2020), 118-137 https://doi.org/10.1504/ijesdf.2020.10025327

[32] Michael Kohn, Mariki M. Eloff, and Jan Eloff, 'Integrated digital forensic process model', *Computers and Security*, 38 (2013), 103–115 https://doi.org/10.1016/j.cose.2013.05.001

[33] Bruce Nikkel, 'NVM Express Drives and Digital Forensics', *Digital Investigation*, 16 (2016), 38–45 https://doi.org/10.1016/j.diin.2016.01.001

and evidence so that this process is an integral part of all digital investigation work and the way in which digital information and evidence are communicated.[34] Details should therefore be documented about all the measures and procedures around which the digital investigation was conducted. As well as all the considerations made, and all the results obtained when the report was prepared during the digital criminal investigation.[35]

Digital Means of Detecting International Crimes

The IT revolution has led to several digital means of detecting previously unknown international crimes. Such means are widely exploited, consisting of a variety of forms, such as memory placed on modern cameras, as well as memory of smartphones and CD-ROMs, as well as cloud services provided by specialized organizations to store vast amounts of data and information.[36] For example, the types of evidence and information received and handled by the Asia-Pacific War Crimes Information Centre are varied. These include individuals' personal data, communication data and document numbers. As well as information on armed groups, militias, command structures and references to specific locations and events. Authorities in those countries provide information from their war crimes investigations that they wish to verify, store or analyze within databases. So, the Asia-Pacific War Crimes Information Centre is a highly secure anti-terrorism database, as well as a special serious organized crime database.[37]

Regarding information and digital evidence obtained from social media platforms, investigative bodies adopt these social platforms to obtain critical digital evidence through the social media platforms' extensive policy control over content moderation. This leads to potential loss of valuable digital information and evidence. In addition, access to deleted content is controlled by the platforms themselves.[38] Although information and digital evidence are generally admissible in criminal evidence, rule 95 of the ICTY Rules of Procedure and Evidence indicates that there are limited rules prohibiting the submission of digital

[34] Radina Stoykova, Stig Andersen, Katrin Franke, and Stefan Axelsson, 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police', *Forensic Science International: Digital Investigation*, 40 (2022), 1-13 https://doi.org/10.1016/j.fsidi.2022.301351

[35] Eoghan Casey, 'Clearly Conveying Digital Forensic Results', *Digital Investigation*, 24 (2018), 1-3 https://doi.org/10.1016/j.diin.2018.03.001

[36] Abdullah Alkhseilat, Tareq Al Billeh, Mohammed Albazi, and Naser Al Ali, 'The Authenticity of Digital Evidence in Criminal Courts: A Comparative Study', *International Journal of Electronic Security and Digital Forensics*, 16.6 (2024), 720–738 https://doi.org/10.1504/ijesdf.2024.142010

[37] Karolina Aksamitowska, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands', Journal of International Criminal Justice, 19.1 (2021), 189–211 https://doi.org/10.1093/jicj/mqab035

[38] Elizabeth White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', *Leiden Journal of International Law*, 37.1 (2024), 228–250 https://doi.org/10.1017/S0922156523000444

information and evidence to international courts. The Special Courts broadly prohibit the submission of digital evidence obtained in ways that raise substantial doubts about its validity and credibility. For whether its acceptance is incompatible with the impartiality of the Court's legal process, or would cause serious harm in the course of the investigation.[39]

The increasing and large number of war crimes trials in European domestic courts, which are based on information and evidence of atrocities committed and shared by different combatants from several States. Therefore, local authorities are under considerable pressure to develop effective methods of collecting, processing, analyzing and exchanging data and evidence from users. The aim of which is to protect their citizens from extremist violence. Although domestic prosecutions in various European States are examples of different tactics, they continue to pave the way for future prosecutions based on the principle of universal jurisdiction.[40] International cooperation is therefore essential for the exchange of information on cross-border cybercrime cases. The global aspect of cybercrime allows such crimes to occur across national borders, regardless of the perpetrator's or victim's whereabouts. Since States with problems of sovereignty and resources could not address those issues on their own, international cooperation within the framework of international criminal policy was strategically necessary and vital in order to combat international and transnational crimes.[41]

Given the nature of digital information and evidence, there are some specific issues that have not been thoroughly addressed in the field of digital information and evidence. So, international investigators must pay special attention in order to ensure the transfer of the reliability and authenticity of digital information and evidence in order to ensure that it is accepted as evidence in criminal investigations. Through the collection and storage of digital information and evidence, the integrity of such information and evidence must be verified.[42] Through reference to Human Rights Council Resolution No. A/HRC/52/62 on (Report of the Independent International Commission of Inquiry on Ukraine) from

---

[39] The ICTY Rules of Procedure and Evidence, Rule 95, 8 July 2015 https://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev50_en.pdf

[40] Chiraz Belhadj Ali, 'International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media', *Groningen Journal of International Law*, 9.1 (2021), 43–59 https://doi.org/10.21827/grojil.9.1.43-59

[41] Widya Setiabudi Sumadinata, 'CYBERCRIME and GLOBAL SECURITY THREATS: A CHALLENGE in INTERNATIONAL LAW', Russian Law Journal, 11.3 (2023), 438-444 https://doi.org/10.52783/rlj.v11i3.1112

[42] Elizabeth White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', *Leiden Journal of International Law*, 37.1 (2024), 228–250 https://doi.org/10.1017/S0922156523000444

27 February 2023 to 31 March 2023 and issued on 15 March 2023. Human rights evidence and fact-finding missions used satellite imagery on Ukraine to document widespread destruction in the residential areas of Ukraine (Mariupol). This is when the International Commission on Human Rights was unable to reach the city because of the conditions of war. Therefore, the use of satellite imagery techniques through sensing data is of great benefit to human rights fact-finding commissions and documentation of any violations of international humanitarian law through access to satellite imagery without the need for war risk.[43] Recent applications of satellite imagery include the use of high-resolution satellite imagery of the Gaza conflict in 2023 in the wake of the renewed war between Israel and Hamas, where a series of maps were used to identify damage through the use of open-source satellite radar data. A set of multidimensional images documenting the destruction in Gaza was obtained.[44]

From past practical experiences, therefore, information and evidence extracted via satellite allows for the identification of objects on Earth with high accuracy, including the depiction of all terrain, vehicles, equipment and persons. Documentation of changes that can be observed in a particular location via satellite may serve over time as independent evidence for documenting violations of human rights and international criminal law. The Berkeley Protocol emphasizes the value and importance of geographical location by determining time location as ways to confirm time and spatial parameters. However, the Berkeley Protocol contains several recommendations rather than mandatory procedures. Investigators in the ICC Prosecutor's Office therefore seek to ensure the validity of evidence and information obtained via satellite. In some cases, the International Criminal Court's criminal expert photographer may be assigned to determine the geographical location of violations of human rights and international criminal law.[45]

Legal and Technical Challenges in Using Digital Evidence to Prosecute International Crimes

The improper use of inadequate technology weakens the right to a fair trial, as provided for in article 6 of the European Convention on Human Rights. And the presumption of innocence is jeopardized during the initial stage of the investigation. Furthermore, the lack of adequate pretrial and trial protection for

[43] A/HRC/52/62, Report of the Independent International Commission of Inquiry on Ukraine. Advance Unedited Version. Human Rights Council. Fifty-second session. 27 February–31 March 2023. Agenda item 4. Human rights situations that require the Council's attention. 15 March 2023. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/coiukraine/A_HRC_52_62_AUV_EN.pdf

[44] Max Tani, Satellite companies are restricting Gaza images. Updated Nov 6, 2023, 5:05am GMT+3. https://www.semafor.com/article/11/05/2023/satellite-companies-are-restricting-gaza-images

[45] María De Arcos Tejerizo, 'Digital Evidence and Fair Trial Rights at the International Criminal Court', *Leiden Journal of International Law*, 36.3 (2023), 749–69 https://doi.org/10.1017/S0922156523000031

accused undermines the credibility of complex digital forensic methods and tools.[46] In addition, the suspect/accused's ability to collect and intercept digital evidence in criminal operations is limited. Therefore, excessive reliance on and improper use of technology, coupled with the suspect's /accused's weak position, may lead to unequal treatment and legal uncertainty in judicial proceedings.[47]

The case law of the European Court of Human Rights (ECtHR) illustrates a comprehensive interpretation of the general principle of a fair trial, allowing for the derivation of two categories of principles to inform the regulation of digital evidence. The initial group is based on the concept of equality of arms and encompasses regulations regarding the assessment of the legality and permissible use of digital evidence, as well as the opportunity to contest it on an informed basis. The second set of digital evidence regulations is based on the presumption of innocence and aims to ensure precise fact-finding while safeguarding innocent suspects from reverse burdens of proof and unfair impacts inherent in technology.[48]

The issue of the reconstruction of the digital crime scene in the courtrooms has raised several legal problems in international and domestic courts. Although digital crime scene reconfiguration can be useful in practice. Particularly, in violations of human rights and international criminal law and prosecution of international crimes. Because it allows the judges of the court to visit the digital crime scene by default which may be too expensive or dangerous to travel to them in person. However, there are several risks to the restructuring of the digital crime scene in the courtrooms related to the accused's rights and their effects on witnesses and fair trial standards.[49]

Indeed, there are many fundamental challenges associated with the use of information and digital evidence to prosecute international crimes. As determining the stages and steps of digital investigation in which the defense must be represented. In addition to the fact that searches and investigations for digital information and data and the re-evaluation and analysis of digital evidence are carried out in modern and scientific methods of investigation. This makes it more difficult to assess digital information and evidence. And if defense counsel does not receive adequate information on the stages of the processing of digital

[46]The European Convention on Human Rights, Article 6, 1950. https://www.echr.coe.int/documents/d/echr/convention_ENG

[47] Radina Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence', *Computer Law & Security Review*, 42 (2021), 1-20 https://doi.org/10.1016/j.clsr.2021.105575

[48] Radina Stoykova, 'A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings', *Computer Law & Security Review*, 55 (2024), 1-16 https://doi.org/10.1016/j.clsr.2024.106040

[49] Sarah Zarmsky, 'Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law', *Journal of International Criminal Justice*, 19.1 (2021), 213–225 https://doi.org/10.1093/jicj/mqab048

evidence and the reliability of such evidence, thus it becomes even more difficult.[50] Therefore, a plan is needed to minimize the change of digital information and to take action to document the actions taken during the initial collection and preservation processes. Original physical storage media, such as laptop, phone and tablet, must be collected. Taking into account the application of strict measures to prevent the corruption of physical objects, and storing the device in a secure location, so that the digital forensic expert can examine it further.[51]

The possibility of the device being connected to a cloud service where data is stored and requested must be taken into account. Access credentials must be obtained and registered if legally feasible. Access credentials must be requested for any platforms to which the device is connected remotely and the data in question are likely to be stored and recorded if legally valid.[52]

The Role of Information and Digital Evidence in Monitoring Violations of Human Rights and International Criminal Law

Open-source digital information and evidence has become widespread in many international conflicts.[53] This, in turn, has led to an evolution in the investigation of international crimes that violate international criminal law. But the international criminal courts have had little opportunity to address the issue of the acceptance of digital information and evidence. With the emergence of online investigations as a necessary investigation in international criminal law. Courts and investigative bodies are facing several forms of digital evidence and information.[54]

Therefore, investigations into violations of human rights and international criminal law using digital information and evidence require the use of many modern digital devices and equipment and computer software. And the compilation, processing and analysis of criminal digital information and evidence for the modelling of investigative procedures. In addition to the use of digital criminal logistics to improve the flow of data and information. And without excluding the use of AI systems and digital criminal logistics in the collection,

---

[50] Radina Stoykova, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations', *Computer Law and Security Review*, 49 (2023), 1-26 https://doi.org/10.1016/j.clsr.2023.105801

[51] Syed Raza Shah Gilani, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan, 'Right of Privacy and the Growing Scope of Artificial Intelligence', *Current Trends in Law and Society*, 3.1 (2023), 1–11 https://doi.org/10.52131/clts.2023.0301.0011

[52] Riccardo Vecellio Segate, 'Cognitive Bias, Privacy Rights, and Digital Evidence in International Criminal Proceedings: Demystifying the Double-Edged AI Revolution', *International Criminal Law Review*, 21.2 (2021), 242–279 https://doi.org/10.1163/15718123-bja10048

[53] Giulia Lanza, 'The Fundamental Role of International (Criminal) Law in the War in Ukraine', *Orbis*, 66.3 (2022), 424-435 https://doi.org/10.1016/j.orbis.2022.05.010

[54] Elizabeth White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', *Leiden Journal of International Law*, 37.1 (2024), 228–250 https://doi.org/10.1017/S0922156523000444

analysis, storage and verification of information and data. And the creation of digital information and evidence that can be used at the International Criminal Court.[55]

The international criminal evidence sometimes contains a lot of audible statements. Therefore, in some cases brought before it, the International Criminal Court has expressed inadmissibility of open-source material based on several anonymous audio statements. Such as those received from NGOs and media sources in view of concerns that raise doubts about the circumstances in which forensic evidence is collected from the crime scene without control from the competent authorities dealing with digital information and evidence.[56] The judiciary relies on the best available evidence under the circumstances surrounding the commission of international crimes. With regard to the International Criminal Guide, there are sometimes many copies of an element or publication through amendments and the addition of irrelevant material. The criminal courts therefore seek to provide the most reliable original versions of digital information and evidence to assist them in deliberating and issuing judicial decisions based on reliable legal information and evidence.[57]

In fact, digital evidence and information are increasingly important in assessing and managing human rights threats such as mitigating mass displacement. However, the current approach to war management needs to cover the contributions of digital evidence and information to support investigations, measures and accountability. And to enforce fundamental human rights and other preventive legal frameworks in order to deter the exploitation of vulnerable societies. The competent authorities must also gather digital evidence and information on grave and serious human rights violations.[58]

Therefore, digital evidence and information available to the public online plays an increasingly pivotal role in human rights investigations. As criminal investigations become more complex, the quality of digital investigation results has decreased. Digital crime investigation and forensic analysis cases include changing crime patterns, the Internet of Things, and the enormous complexity of the investigation. After moving into the Internet of Everything era, a variety of IoT-based forensic methods emerged, including multilateral forensic analysis,

[55] Sergey Zuev and Dmitry Bakhteev, 'Digital Forensic Logistics: The Basics of Scientific Theory', *International Journal of Law and Society*, 4.2 (2021), 83-88 https://doi.org/10.11648/j.ijls.20210402.14
[56] Naeem AllahRakha, 'Transformation of Crimes (Cybercrimes) in Digital Age', *International Journal of Law and Policy*, 2.2 (2024), 1-19 https://doi.org/10.59022/ijlp.156
[57] Matthew Gillett, and Wallace Fan, 'Expert Evidence and Digital Open Source Information', Journal of International Criminal Justice, 21.4 (2023), 661–693 https://doi.org/10.1093/jicj/mqad050
[58] Srinivasa Murthy Pedapudi, and Nagalakshmi Vadlamani, 'Digital Forensics Approach for Handling Audio and Video Files', *Measurement: Sensors*, 29 (2023), 1-5 https://doi.org/10.1016/j.measen.2023.100860

such as sensor equipment, communications equipment, automobiles and drones, as well as the relationship between smart groups and smart structures.[59]

Clearly, digital information and evidence represents a legal challenge to the international criminal justice system. By analyzing the current legal framework governing information and digital evidence in international criminal law, the International Criminal Court's legal organization did not address the definition of digital information and evidence.[60] And the Rules for the Admission and Exclusion of Information and Evidence before the International Criminal Court. As well as the credibility, reliability and evidentiary value of digital information and evidence in criminal matters. In addition, the potential risks involved in the acceptance and use of digital information and evidence in the International Criminal Court's trial proceedings are also added.[61]

For example, in its report No. A/HRC/42/CRP.3 of the United Nations Commission on Human Rights on the economic interests of the Myanmar army on 16 September 2019. The Independent International Fact-Finding Mission on Myanmar used open-sources, direct sources and other information in the investigation process, findings and conclusions. The final report of the fact-finding mission was one of the factors that led to the Human Rights Council's establishment of an independent investigative mechanism in Myanmar. And the fact-finding mission was also forced to hand over evidence and information, including the contents of the open-source investigation. The fact-finding mission's reports were also relied upon in its case (The Gambia) before the International Court of Justice against Myanmar for its violation of the Convention on the Prevention of the Crime of Genocide.[62]

Examples include visual reports in digital platforms used as illustrative evidence in (Prosecutor vs. Ahmed Al-Faki Al-Mahdi), in which the ICC rendered a final judgement on 24 March 2016, stating that "the most repayable evidence provided by the Prosecutor in connection with the destruction of buildings (Buildings/building) in Timbuktu and damage thereto from 30 June 2012 to 11 July 2012, approximately as follows: a recorded video of the destruction and its aftermath, witness statements with good knowledge of the relevant events

[59] Daragh Murray, Yvonne McDermott, and K Alexa Koenig, 'Mapping the Use of Open Source Research in UN Human Rights Investigations', *Journal of Human Rights Practice*, 14.2 (2022), 554–581 https://doi.org/10.1093/jhuman/huab059

[60] Renata Marcinauskaitė, and Yulia Razmetaeva, 'Privacy Protection In The Digital Age: A Criminal Law Perspective', *International Comparative Jurisprudence*, 7.2 (2021), 153–168 https://doi.org/10.13165/j.icj.2021.12.004

[61] Chiara Ragni, 'Digital Evidence In International Criminal Proceedings And Human Rights Challenges', *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7 (2023), 1–16 https://doi.org/10.25234/eclic/28255

[62] A/HRC/42/CRP.3, Full report: the economic interests of the Myanmar military https://www.ohchr.org/en/hr-bodies/hrc/myanmar-ffm/economic-interests-myanmar-military

(witnesses P-65, P-66, P-114, P-125 and P-151), images, including satellite images of premises/buildings before and after their destruction (in part), documents issued by the financial authorities, expert analyses, media reports, statements and reports issued by international organizations, including UNESCO".[63]

Prosecutor v. Saleem Jameel Ayyash, Hasan Habeeb Mare'i, Hussein Hasan Anisi, Asad Hasan Sabra. At the Special Tribunal for Lebanon dated 28 August 2020, the Special Tribunal for Lebanon was based (Trial Chamber), Netherlands, "in primarily explaining the evidence linking Mr. Ayyash to red phone 741, without which there would have been no evidence linking him to the attack (para. 543 of the summary judgement; para. 6714 of the actual judgement). The red phones tracked Mr. Hariri's movements and were prepared to carry out the attack when the convoy passed (para. 6804 of the actual judgement), thereby establishing the criminal act".[64]

The report on the detailed results of the Independent International Commission of Inquiry on Protests in the Occupied Palestinian Territory, No. A/HRC/40/CRP.2, dated 18 March 2019, so that "the Committee gathered more than 8000 documents from a wide range of sources, including statements, medical reports, space images, social media, videos, photographs and opinions of legal experts, related to events at the sites of demonstrations. The Committee also reviewed publicly available information, including information from the Government of Israel's official websites. The Commission considered the following sources of direct information: video material, documented photographs and satellite imagery".[65]

More importantly, it is the criminal judge who assesses the acceptance and evidentiary value of digital information and evidence during trials before the International Criminal Court. However, in order to enhance judicial evaluation of the facts in relation to digital information and evidence, digital investigation procedures must ensure at least the minimum quality of digital information and evidence. And that they are admissible in evidence and have been properly and legally obtained, requiring adherence to criminal standards and procedures. As well as, verification of the quality standards of digital investigation on which each State's jurisdiction depends. However, proving the reliability of digital

[63] Prosecutor v. Ahmad Al Faqi Al Mahdi at the International Criminal Court https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/Al-MahdiEng.pdf

[64] The Prosecutor v. Salim Jamil Ayyash, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra https://www.internationalcrimesdatabase.org/Case/3314/The-Prosecutor-v-Salim-Jamil-Ayyash,-Hassan-Habib-Merhi,/

[65] A/HRC/40/CRP.2, Human Rights Council Fortieth session 25 February–22 March 2019 Agenda item 7 Human rights situation in Palestine and other occupied Arab territories Report of the detailed findings of the independent international Commission of inquiry on the protests in the Occupied Palestinian Territory, 18 March 2019 https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf

information and evidence is a factor affecting the evidence value of the digital evidence before the International Criminal Court.[66]

However, the criteria considered by international tribunals' judicial chambers in assessing the acceptability and weight of digital information and evidence in criminal proceedings remain unclear. Because the full scope of the role of digital information and evidence in evidence is not addressed. The ambiguity of those decisions concerning digital information and evidence is due to the way in which these information and digital evidence are assessed and differ from one chamber to another. In addition, international criminal judges are not experts in handling digital information and evidence.[67]

Yet, in some critical cases in which satellite imagery is obtained, there is a problem with the reliability of such images before the International Criminal Court (ICC). Is the Court obliged to validate them? Which means that there is sufficient evidence about the investigation of human rights violations. Therefore, the authentication of satellite images by the International Criminal Court (ICC) requires that the filmed location and the date of the photograph's recording be determined so that this location can be spatially linked to human rights violations. Thus, create a temporal link between satellite images and cases of violations of human rights and international criminal law raised in the indictment submitted to the Court. Satellite images can be validated by demonstrating the integrity of data and technically generated visual content. And using other reliable evidence such as oral evidence that can confirm satellite image content. Once satellite images have been validated, their reliability must be established to verify violations of human rights and international criminal law by assessing the clarity and accuracy of satellite images.[68]

The Intersection of Digital Evidence and Privacy Rights in Human Rights Violations Investigations

The right to privacy is a fundamental human right, it is one of the important elements of the right to privacy is the right to protect individuals' personal data in accordance with personal data protection laws. These laws have become increasingly important when using digital ICT investigations, as confirmed in UN

[66] Stoykova, Radina, and Katrin Franke, 'Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations', *Forensic Science International: Digital Investigation*, 45 (2023), 1-11 https://doi.org/10.1016/j.fsidi.2023.301554

[67] Beata Stępień-Załucka, 'Drones, Real Estate Video Surveillance, and Neighbourhood Right to Privacy – The Potential Area of Normative Impact from the Perspective of the Polish Law', *Journal of Intelligent and Robotic Systems: Theory and Applications*, 106.1 (2022), 1-8 https://doi.org/10.1007/s10846-022-01693-2

[68] Adaena Sinclair-Blakemore, 'The Admission of New Prosecutorial Evidence in International Criminal Retrials', *Journal of International Criminal Justice*, 21.4 (2023), 903–930 https://doi.org/10.1093/jicj/mqad042

Human Rights Council Report No. A/HRC/39/29 on the Right to Privacy in the Digital Age, issued on 3rd August 2018.[69]

Therefore, the right to privacy is often viewed as a fundamental human right, although not explicitly mentioned, it can be inferred by reference to article 12 of the Universal Declaration of Human Rights. Which states: "No one shall be subjected to arbitrary interference with his privacy".[70] According to article 6 of the European Convention on Human Rights, in addition to articles 47 and 48 of the Charter of Fundamental Rights of the European Union, it must be ascertained that "the evidence obtained during cross-border investigations shall not be used unfairly or unlawfully".[71]

The relationship between privacy protection and personal data protection presents legal and scholarly complexities. The law has transitioned from a traditional monistic approach to privacy rights, which encompassed personal information protection, to a dualistic framework that distinguishes between privacy protection and personal information protection. However, when the private information within the privacy realm pertains to personal data, the dualistic protection is not total but rather more nuanced. Privacy is inherently an intrinsic right that safeguards dignity and liberty.[72]

Accordingly, the majority of the world's nations have recognized the right to privacy in the digital space, so that the right to privacy is one of the most important human rights. It guarantees humans a free and secure life, which is a basis for the protection of their dignity and independence.[73] The right to privacy continues to be the subject of international controversy and debate over its definition and characteristics, considering that it is essentially linked to a relative

[69] A/HRC/39/29, Human Rights Council, The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf

[70] The Universal Declaration of Human Rights, Article 12, 1948 https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf

[71] The European Convention on Human Rights, Article 6, 1950. https://www.echr.coe.int/documents/d/echr/convention_ENG . The Charter of Fundamental Rights of the European Union, Articles 47 and 48, 18 December 2000 https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[72] Zhilong Guo, Jie Hao, and Lewis Kennedy, 'Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law', *Computer Law & Security Review*, 52 (2024), 105928 https://doi.org/10.1016/j.clsr.2023.105928

[73] Tareq Al-Billeh, 'Legal framework for protecting the right to private life in the digital space: the extent to which Jordanian constitution and legislation takes into account international requirements', *Revista de Investigaciones Constitucionales*, 11.1 (2024), 1–23 http://dx.doi.org/10.5380/rinc.v11i1.90631

and flexible idea. The right to privacy is regarded as an international humanitarian right at the international and national levels.[74]

Often, States' Governments may violate the right to privacy under the cover of legality, so that the issue of control over personal data and information raises several legal problems. Censorship of personal data and information is often justified on the basis of maintaining public order in the State and maintaining national security. The State may intentionally censor personal data and information in order to extend its control to individuals and institutions within the State.[75] The right to privacy therefore constitutes a guarantee against arbitrary State control by preventing States' Governments from conducting illegal surveillance. To strengthen democratic norms, the right to privacy helps to preserve civil liberties. Data and personal information of individuals are collected and disseminated largely due to technological advances. Individuals therefore need to protect their privacy in order to prevent any breach of personal information and data, illegal digital surveillance and identity theft.[76]

Therefore, the establishment of a permanent mechanism of investigation of violations of human rights and international criminal law would enhance the collection and use of digital information and evidence in various aspects of the international criminal justice system. In particular, in the area of open-source evidence, the use of digital information and evidence enhances international criminal justice. Given the recent use of open-source evidence produced by users before international criminal tribunals, although scientific and technical progress has been made by court investigative bodies, some challenges remain with regard to the use of digital information and evidence in demonstration. The courts' investigative mechanism could lead to the unification of international standards in the use of digital information and evidence. Thereby, improving the quality of international criminal investigations conducted by specialized investigative bodies and activating prosecutions.[77]

In fact, individuals use digital media as a means of storing vast amounts of information about their daily lives. Due to the widespread use of digital devices, law enforcement agents often encounter digital crime theatres, where large files

---

[74] Oliver Diggelmann, and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right', *Human Rights Law Review*, 14.3 (2014), 441–458 https://doi.org/10.1093/hrlr/ngu014

[75] Alexander Heinze, 'Evidence Illegally Obtained by Private Investigators and Its Use before International Criminal Tribunals', *New Criminal Law Review*, 24.2 (2021), 212–253 https://doi.org/10.1525/nclr.2021.24.2.212

[76] Özgür Heval Çınar, 'The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age', The International Journal of Human Rights, 25.1 (2020), 26-51 https://doi.org/10.1080/13642987.2020.1747443

[77] Manjula Raghav and Sanjana Sharma Marwaha, 'Indian Legal Framework on the Right to Privacy in Cyberspace-Issues and Challenges', *Fiat Justisia: Jurnal Ilmu Hukum*, 17.1 (2023), 1–16 https://doi.org/10.25041/fiatjustisia.v17no1.2667

exist. Traditionally, the common practice in digital forensic medicine has been to confiscate all physical storage devices in order to examine images obtained from such devices.[78] However, the technology has faced criticism for fears that it could disproportionately violate the accused's privacy and disrupt companies' business operations by collecting all material. The accused is therefore entitled to be protected from intrusive searches and seizures by government agents.[79]

Therefore, excessive restrictions on the search and seizure of digital information would reduce the effectiveness of investigations and potentially hinder the discovery of critical evidence. It was therefore necessary to develop a rational approach capable of reconciling conflicting principles of human rights protection and conducting a thorough investigation. Currently, there have been few research efforts to address field operations specifically related to this issue in the area of digital forensics.[80]

Hence, international investigators must be alerted that continuous monitoring and long-term collection and preservation of personal data may require in some laws of the world's States permission or legal authorization with guarantees for violation of privacy. For example, by reference to Chapter 12 of the Data Protection Act 2018, Part 3, Chapter 3, Section 39 (1) In the United Kingdom of Great Britain and Northern Ireland, it stipulated that "Personal data processed for law enforcement purposes must not be kept for longer than is necessary for the purpose for which they are processed. Personal data can only be collected for specific, explicit and legitimate purposes, must be limited to information necessary for the purpose for which they are collected and must remain identifiable only as long as necessary for the purposes of collection".[81]

Through reference to recent legislation on the protection of personal data in some Arab countries. Article 4 of Jordan's Personal Data Protection Act No. 24 of 2023 provides that: "Subject to article 6 of this Act: - a. Every natural person has the right to the protection of his data and may be treated only after obtaining the prior consent of the person concerned or in legally authorized circumstances." However, the Act provides in article 15 that: "a. Data may not be transferred to any person outside the Kingdom, including the recipient, if the level of protection

[78] Tareq Al-Billeh, Ruba Hmaidan, Ali Al-Hammouri, Mohammed AL Makhmari, 'The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards', *Jurnal Media Hukum*, 31.2 (2024), 333-350 https://doi.org/10.18196/jmh.v31i2.23480

[79] Ilyoung Hong, Hyeon Yu, Sangjin Lee, and Kyungho Lee, 'A New Triage Model Conforming to the Needs of Selective Search and Seizure of Electronic Evidence', *Digital Investigation*, 10.2 (2013), 175–92 https://doi.org/10.1016/j.diin.2013.01.003

[80] Syed Raza Shah Gilani, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan, 'Right of Privacy and the Growing Scope of Artificial Intelligence', *Current Trends in Law and Society*, 3.1 (2023), 1–11 https://doi.org/10.52131/clts.2023.0301.0011

[81] The Data Protection Act 2018, part 3, chap. 3, sect. 39 (1) in the United Kingdom of Great Britain and Northern Ireland, Chapter 12 https://www.legislation.gov.uk/ukpga/2018/12/part/3

afforded to such data is lower than that provided for in this Act except in the following cases: 1. Regional or international judicial cooperation under international conventions or treaties in force in the Kingdom. 2. International or regional cooperation with international or regional bodies, organizations or agencies involved in combating or prosecuting crime of all kinds".[82]

With regard to the relationship between the right to privacy and the right to protection of personal data when investigating violations of human rights and criminal law. The International Criminal Court must set out the legal limits of the right to privacy and the right to the protection of personal data in order to strike a balance between those rights. Each right has objectives, purposes and substance different from the other right. The International Criminal Court must make an effort to clarify whether persons are entitled to the protection of the right to privacy and the right to the protection of personal data.[83] A modern practical application to violate the right to privacy using modern technology is the use of cameras on drones, which allow for the recording of photographs and videos containing accurate details of controlled property. In addition to monitoring the movements of private individuals, which may document violations of human rights and international criminal law. This type of use of modern technologies may therefore be linked to the violation of the personal rights of owners of those properties that are monitored, in addition to restricting individuals' freedom of movement and privacy.[84]

Furthermore, digital evidence and information have shown their effectiveness in domestic prosecutions of core international crimes. In addition, in the absence of strict rules on the admissibility of evidence and digital information, the Court has the right to accept any digital evidence that contributes to its objective of detecting international crimes. However, the video or photo has to meet certain requirements regarding the origin and date of creation. When international and local authorities face challenges in dealing with digital evidence and information, assistance is sought from the United Nations body or the European Union's authorities. Furthermore, forensic experts regularly contribute to supporting cybercrime units in assessing the validity and reliability of digital evidence and information by verifying that digital evidence and information submitted to the International Criminal Court has considerable evidentiary value in criminal

[82] Jordan's Personal Data Protection Act No. 24 of 2023, Article 4 https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf

[83] Valentin M. Pfisterer, 'The Right to Privacy—a Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy', *German Law Journal*, 20.5 (2019), 722–733 https://doi.org/10.1017/glj.2019.57

[84] Beata Stępień-Załucka, 'Drones, Real Estate Video Surveillance, and Neighbourhood Right to Privacy – The Potential Area of Normative Impact from the Perspective of the Polish Law', *Journal of Intelligent and Robotic Systems: Theory and Applications*, 106.1 (2022), 1-8 https://doi.org/10.1007/s10846-022-01693-2

evidence and that digital evidence and information have not been manipulated and falsified.[85]

4. Conclusion

The use of digital information in investigating human rights violations and international criminal law has grown significantly in recent years. Digital tools such as the Internet, social media, and satellite imagery are increasingly employed to collect information and evidence against suspected individuals involved in serious international crimes. These crimes often span a global geographic scope, and digital evidence has become a crucial component in identifying suspects, confronting them with evidence, and referring them to international courts for justice. The reliance on digital evidence is expected to expand further, as it offers an efficient and reliable means to document international crimes and hold perpetrators accountable. However, digital evidence should not be viewed as a singular solution to the challenges of criminal investigations or as a substitute for addressing human rights violations comprehensively. Courts in some jurisdictions have raised concerns about the authenticity and reliability of reports based on digital evidence, citing insufficient scientific validation. To address these concerns, international charters are needed to standardize the use of digital evidence in investigations, ensuring both legitimacy and the protection of privacy. These charters should outline mechanisms for using digital evidence to monitor and document crimes such as genocide, war crimes, and crimes against humanity while upholding fundamental human rights.

Refrences

A/HRC/39/29, Human Rights Council, The right to privacy in the digital age Report of the United Nations High Commissioner for Human Rights https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf

A/HRC/40/CRP.2, Human Rights Council Fortieth session 25 February–22 March 2019 Agenda item 7 Human rights situation in Palestine and other occupied Arab territories Report of the detailed findings of the independent international Commission of inquiry on the protests in the Occupied Palestinian Territory, 18 March 2019 https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf

A/HRC/42/CRP.3, Full report: the economic interests of the Myanmar military https://www.ohchr.org/en/hr-bodies/hrc/myanmar-ffm/economic-interests-myanmar-military

[85] Chiara Ragni, 'Digital Evidence In International Criminal Proceedings And Human Rights Challenges', *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7 (2023), 1–16 https://doi.org/10.25234/eclic/28255

A/HRC/52/62, Report of the Independent International Commission of Inquiry on Ukraine. Advance Unedited Version. Human Rights Council. Fifty-second session. 27 February–31 March 2023. Agenda item 4. Human rights situations that require the Council's attention. 15 March 2023. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/coiukraine/A_HRC_52_62_AUV_EN.pdf

Agrawal, Animesh Kumar, Aman Sharma, Sumitra Ranjan Sinha, and Pallavi Khatri, 'Forensic of an Unrooted Mobile Device', *International Journal of Electronic Security and Digital Forensics*, 12.1 (2020), 118-137 https://doi.org/10.1504/ijesdf.2020.10025327

Akhlaq, Muhammad, Hafiz Adil Jahangir, and Hamzullah Khan, 'Defending the Right to Privacy in the Digital Age', *Journal of Policy Research*, 8.4 (2022), 534–538 https://doi.org/10.61506/02.00006

Akosu, Nicholas, and Ali Selamat, 'Incorporating Language Identification in Digital Forensics Investigation Framework', *Studies in Computational Intelligence*, 555 (2014), 63–78 https://doi.org/10.1007/978-3-319-05885-6_4

Aksamitowska, Karolina, 'Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands', *Journal of International Criminal Justice*, 19.1 (2021), 189–211 https://doi.org/10.1093/jicj/mqab035

Al-Billeh, Tareq, 'Legal framework for protecting the right to private life in the digital space: the extent to which Jordanian constitution and legislation takes into account international requirements', *Revista de Investigaciones Constitucionales*, 11.1 (2024), 1–23 http://dx.doi.org/10.5380/rinc.v11i1.90631

Al-Billeh, Tareq, Ruba Hmaidan, Ali Al-Hammouri, Mohammed AL Makhmari, 'The Risks of Using Artificial Intelligence on Privacy and Human Rights: Unifying Global Standards', *Jurnal Media Hukum*, 31.2 (2024), 333-350 https://doi.org/10.18196/jmh.v31i2.23480

Alkhseilat, Abdullah, Tareq Al Billeh, Mohammed Albazi, and Naser Al Ali, 'The Authenticity of Digital Evidence in Criminal Courts: A Comparative Study', *International Journal of Electronic Security and Digital Forensics*, 16.6 (2024), 720–738 https://doi.org/10.1504/ijesdf.2024.142010

AllahRakha, Naeem, 'Transformation of Crimes (Cybercrimes) in Digital Age', *International Journal of Law and Policy*, 2.2 (2024), 1-19 https://doi.org/10.59022/ijlp.156

Arcos Tejerizo, María, 'Digital Evidence and Fair Trial Rights at the International Criminal Court', *Leiden Journal of International Law*, 36.3 (2023), 749–69 https://doi.org/10.1017/S0922156523000031

Barten, Dennis G., Derrick Tin, Fredrik Granholm, Diana Rusnak, Frits van Osch, and Gregory Ciottone. 'Attacks on Ukrainian Healthcare Facilities during the First Year of the Full-Scale Russian Invasion of Ukraine', *Conflict and Health*, 17.1 (2023), 1-7 https://doi.org/10.1186/s13031-023-00557-2

Belhadj Ali, Chiraz, 'International Crimes in the Digital Age: Challenges and Opportunities Shaped by Social Media', *Groningen Journal of International Law*, 9.1 (2021), 43–59 https://doi.org/10.21827/grojil.9.1.43-59

Brown, Cameron, 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology*, 9.91 (2015), 55–119 https://doi.org/10.5281/zenodo.22387

Buckley, Peter J., Peter Enderwick, Linda Hsieh, and Oded Shenkar, 'International business theory and the criminal multinational enterprise', *Journal of World Business*, 59.5 (2024), 1-11 https://doi.org/10.1016/j.jwb.2024.101553

Casey, Eoghan, 'Clearly Conveying Digital Forensic Results', *Digital Investigation*, 24 (2018), 1-3 https://doi.org/10.1016/j.diin.2018.03.001

Casey, Eoghan, Lam Nguyen, Jeffrey Mates, and Scott Lalliss, 'Crowdsourcing Forensics: Creating a Curated Catalog of Digital Forensic Artifacts', *Journal of Forensic Sciences*, 67.5 (2022), 1846–1857 https://doi.org/10.1111/1556-4029.15053

Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, and Constantinos Patsakis, 'SoK: Cross-Border Criminal Investigations and Digital Evidence', *Journal of Cybersecurity*, 8.1 (2022), 1-18 https://doi.org/10.1093/cybsec/tyac014

Çınar, Özgür Heval, 'The Current Case Law of the European Court of Human Rights on Privacy: Challenges in the Digital Age', *The International Journal of Human Rights*, 25.1 (2021), 26-51 https://doi.org/10.1080/13642987.2020.1747443

Diggelmann, Oliver, and Maria Nicole Cleis, 'How the Right to Privacy Became a Human Right', *Human Rights Law Review*, 14.3 (2014), 441–458 https://doi.org/10.1093/hrlr/ngu014

Fomina, Tatiana, and Oleksii Rachinskyi, 'Electronic Evidence in Criminal Proceedings: Problematic Issues of Theory and Practice', *Bulletin of Kharkiv National University of Internal Affairs*, 102.3 (2023), 207–220 https://doi.org/10.32631/v.2023.3.43

Gilani, Syed Raza Shah, Ali Mohammed Al-Matrooshi, and Muhammad Haroon Khan, 'Right of Privacy and the Growing Scope of Artificial Intelligence', *Current Trends in Law and Society*, 3.1 (2023), 1–11 https://doi.org/10.52131/clts.2023.0301.0011

Gillett, Matthew, and Wallace Fan, 'Expert Evidence and Digital Open Source Information', *Journal of International Criminal Justice*, 21.4 (2023), 661–693 https://doi.org/10.1093/jicj/mqad050

Gruber, Jan, Christopher J. Hargreaves, and Felix C. Freiling, 'Contamination of Digital Evidence: Understanding an Underexposed Risk', *Forensic Science International: Digital Investigation*, 44 (2023), 1-10 https://doi.org/10.1016/j.fsidi.2023.301501

Guo, Zhilong, Jie Hao, and Lewis Kennedy, 'Protection path of personal data and privacy in China: Moving from monism to dualism in civil law and then in criminal law', *Computer Law & Security Review*, 52 (2024), 105928 https://doi.org/10.1016/j.clsr.2023.105928

Gutsalyuk, Mykhaylo, and P. ANTONIUK, 'Procedural Capacity of Use Electronic (Digital) Information as Evidence in Criminal Proceedings', *INFORMATION AND LAW*, 2.41 (2022), 116–22 https://doi.org/10.37750/2616-6798.2022.2(41).270373

Heinze, Alexander, 'Evidence Illegally Obtained by Private Investigators and Its Use before International Criminal Tribunals', *New Criminal Law Review*, 24.2 (2021), 212–253 https://doi.org/10.1525/nclr.2021.24.2.212

Hong, Ilyoung, Hyeon Yu, Sangjin Lee, and Kyungho Lee, 'A New Triage Model Conforming to the Needs of Selective Search and Seizure of Electronic Evidence', *Digital Investigation*, 10.2 (2013), 175–92 https://doi.org/10.1016/j.diin.2013.01.003

Horsman, Graeme, 'Digital Evidence and the Crime Scene', *Science & Justice*, 61.6 (2021), 761–770 https://doi.org/10.1016/j.scijus.2021.10.003

Horsman, Graeme, 'Digital Evidence Strategies for Digital Forensic Science Examinations', *Science & Justice*, 63.1 (2023), 116–126 https://doi.org/10.1016/j.scijus.2022.11.004

Jordan's Personal Data Protection Act No. 24 of 2023, Article 4 https://www.modee.gov.jo/ebv4.0/root_storage/en/eb_list_page/pdpl.pdf

Kohn, Michael, Mariki M. Eloff, and Jan Eloff, 'Integrated digital forensic process model', *Computers and Security*, 38 (2013), 103–115 https://doi.org/10.1016/j.cose.2013.05.001

Lanza, Giulia, 'The Fundamental Role of International (Criminal) Law in the War in Ukraine', *Orbis*, 66.3 (2022), 424-435 https://doi.org/10.1016/j.orbis.2022.05.010

MacLean, Ken, 'Interactive Digital Platforms, Human Rights Fact Production, and the International Criminal Court', *Journal of Human Rights Practice*, 15.1 (2023), 84–99 https://doi.org/10.1093/jhuman/huac062

Marcinauskaitė, Renata, and Yulia Razmetaeva, 'Privacy Protection In The Digital Age: A Criminal Law Perspective', *International Comparative Jurisprudence*, 7.2 (2021), 153–168 https://doi.org/10.13165/j.icj.2021.12.004

Miller, Christa, 'A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point', *Forensic Science International: Synergy*. 6 (2023), 1-22 https://doi.org/10.1016/j.fsisyn.2022.100296

Murray,Daragh, Yvonne McDermott, and K Alexa Koenig, 'Mapping the Use of Open Source Research in UN Human Rights Investigations', *Journal of Human Rights Practice*, 14.2 (2022), 554–581 https://doi.org/10.1093/jhuman/huab059

Nikkel, Bruce, 'NVM Express Drives and Digital Forensics', *Digital Investigation*, 16 (2016), 38–45 https://doi.org/10.1016/j.diin.2016.01.001

Office of the United Nations High Commissioner for Human Rights, 'Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal', *Human Rights and Humanitarian Law*, (2022), 1-102 https://doi.org/10.18356/9789210053433

Pedapudi, Srinivasa Murthy, and Nagalakshmi Vadlamani, 'Digital Forensics Approach for Handling Audio and Video Files', *Measurement: Sensors*, 29 (2023), 1-5 https://doi.org/10.1016/j.measen.2023.100860

Pfisterer, Valentin M, 'The Right to Privacy—a Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy', *German Law Journal*, 20.5 (2019), 722–733 https://doi.org/10.1017/glj.2019.57

Prosecutor v. Ahmad Al Faqi Al Mahdi at the International Criminal Court https://www.icc-cpi.int/sites/default/files/CaseInformationSheets/Al-MahdiEng.pdf

Prysiazhniuk, Ivan, 'Use of digital evidence in criminal process: some issues of right to privacy protection', *Visegrad Journal on Human Rights*, 5 (2023), 81-88 https://doi.org/10.61345/1339-7915.2023.5.11

Raghav, Manjula and Sanjana Sharma Marwaha, 'Indian Legal Framework on the Right to Privacy in Cyberspace-Issues and Challenges', *Fiat Justisia: Jurnal Ilmu Hukum*, 17.1 (2023), 1–16 https://doi.org/10.25041/fiatjustisia.v17no1.2667

Ragni, Chiara, 'Digital Evidence in International Criminal Proceedings and Human Rights Challenges', *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 7 (2023), 1–16 https://doi.org/10.25234/eclic/28255

Reedy, Paul, 'Digital Evidence Review 2016–2019', *Forensic Science International: Synergy*, 2 (2020) 489–520 https://doi.org/10.1016/j.fsisyn.2020.01.015

Segate, Riccardo Vecellio, 'Cognitive Bias, Privacy Rights, and Digital Evidence in International Criminal Proceedings: Demystifying the Double-Edged AI Revolution', *International Criminal Law Review*, 21.2 (2021), 242–279 https://doi.org/10.1163/15718123-bja10048

Sergey Zuev and Dmitry Bakhteev, 'Digital Forensic Logistics: The Basics of Scientific Theory', *International Journal of Law and Society*, 4.2 (2021), 83-88 https://doi.org/10.11648/j.ijls.20210402.14

Sinclair-Blakemore, Adaena, 'The Admission of New Prosecutorial Evidence in International Criminal Retrials', *Journal of International Criminal Justice*, 21.4 (2023), 903–930 https://doi.org/10.1093/jicj/mqad042

Slipeniuk, Tetiana, Mykola Yankovyi, Viktor Nikitenko, Oleksandr Manzhai, and Yuliia Tiuria, 'Problematic Issues of Using Electronic Evidence in Criminal Proceedings (SDG's)', *Journal of Lifestyle and SDGs Review*, 4.1 (2024), 1-15 https://doi.org/10.47172/2965-730X.SDGsReview.v4.n00.pe01867

Stępień-Załucka, Beata, 'Drones, Real Estate Video Surveillance, and Neighbourhood Right to Privacy – The Potential Area of Normative Impact from the Perspective of the Polish Law', *Journal of Intelligent and Robotic Systems: Theory and Applications*, 106.1 (2022), 1-8 https://doi.org/10.1007/s10846-022-01693-2

Stoykova, Radina, and Katrin Franke, 'Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations', *Forensic Science International: Digital Investigation*, 45 (2023), 1-11 https://doi.org/10.1016/j.fsidi.2023.301554

Stoykova, Radina, 'A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings', *Computer Law & Security Review*, 55 (2024), 1-16 https://doi.org/10.1016/j.clsr.2024.106040

Stoykova, Radina, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence', *Computer Law & Security Review*, 42 (2021), 1-20 https://doi.org/10.1016/j.clsr.2021.105575

Stoykova, Radina, Stig Andersen, Katrin Franke, and Stefan Axelsson, 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police', *Forensic Science International: Digital Investigation*, 40 (2022), 1-13 https://doi.org/10.1016/j.fsidi.2022.301351

Stoykova, Radina, 'The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations', *Computer Law and Security Review*, 49 (2023), 1-26 https://doi.org/10.1016/j.clsr.2023.105801

Struijk, Mylène, Spyros Angelopoulos, Carol X.J. Ou, and Robert M. Davison, 'Navigating Digital Transformation through an Information Quality Strategy: Evidence from a Military Organisation', *Information Systems Journal*, 33.4 (2023), 912–952 https://doi.org/10.1111/isj.12430

Sumadinata, Widya Setiabudi, 'Cybercrime And Global Security Threats: A Challenge In International Law', *Russian Law Journal*, 11.3 (2023), 438-444 https://doi.org/10.52783/rlj.v11i3.1112

Sunardi, Sunardi, and Ridho Surya Kusuma, 'Digital Evidence Security System Design Using Blockchain Technology', *International Journal of Safety and Security Engineering*, 13.1 (2023), 159–165 https://doi.org/10.18280/ijsse.130118

Tani, Max, Satellite companies are restricting Gaza images. Updated Nov 6, 2023, 5:05am GMT+3. https://www.semafor.com/article/11/05/2023/satellite-companies-are-restricting-gaza-images

The Charter of Fundamental Rights of the European Union, Articles 47 and 48, 18 December 2000 https://www.europarl.europa.eu/charter/pdf/text_en.pdf

The Data Protection Act 2018, part 3, chap. 3, sect. 39 (1) in the United Kingdom of Great Britain and Northern Ireland, Chapter 12 https://www.legislation.gov.uk/ukpga/2018/12/part/3

The European Convention on Human Rights, Article 6, 1950. https://www.echr.coe.int/documents/d/echr/convention_ENG

The ICTY Rules of Procedure and Evidence, Rule 95, 8 July 2015 https://www.icty.org/x/file/Legal%20Library/Rules_procedure_evidence/IT032Rev50_en.pdf

The Prosecutor v. Salim Jamil Ayyash, Hassan Habib Merhi, Hussein Hassan Oneissi, Assad Hassan Sabra https://www.internationalcrimesdatabase.org/Case/3314/The-Prosecutor-v-Salim-Jamil-Ayyash,-Hassan-Habib-Merhi,/

The Universal Declaration of Human Rights, Article 12, 1948 https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/eng.pdf

Tsai, Fu-Ching, 'The Application of Blockchain of Custody in Criminal Investigation Process', *Procedia Computer Science*, 192 (2021), 2779-2788 https://doi.org/10.1016/j.procs.2021.09.048

White, Elizabeth, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', *Leiden Journal of International Law*, 37.1 (2024), 228–250 https://doi.org/10.1017/S0922156523000444

Zarmsky, Sarah, 'Why Seeing Should Not Always Be Believing: Considerations Regarding the Use of Digital Reconstruction Technology in International Law', *Journal of International Criminal Justice*, 19.1 (2021), 213–225 https://doi.org/10.1093/jicj/mqab048