The Rights to Privacy and Data Protection in Times of Armed Conflict

Edited by
Russell Buchan
Asaf Lubin

CCDCOE

The Rights to Privacy and Data Protection in Times of Armed Conflict

Russell Buchan and Asaf Lubin (Eds.)

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

The Rights to Privacy and Data Protection in Times of Armed Conflict

ISBN (print): 978-9916-9565-6-4
ISBN (pdf): 978-9916-9565-7-1

2022 © NATO CCDCOE Publications
NATO CCDCOE Publications
Filtri tee 12, 10132 Tallinn, Estonia
Phone: +372 717 6800
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Cover design & content layout: Stuudio Stuudio

Chapter 12

Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study

Asaf Lubin[1]

INTRODUCTION

On 16 February 2022, Robert Mardini, the Director-General of the International Committee of the Red Cross (ICRC) issued an open letter in which he apologized for failing to adequately protect the servers that stored the personal data of over 515,000 people worldwide.[2] This cyber attack first began on 9 November 2021 and involved a nation State that exploited a known but unpatched vulnerability in a web-based office communications management program that the Red Cross was internally using for

1 Dr. Asaf Lubin is an Associate Professor of Law at Indiana University Maurer School of Law and a Fellow at IU's Center for Applied Cybersecurity Research. He is additionally an Affiliated Fellow at Yale Law School's Information Society Project, a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University, and a visiting Scholar at the Hebrew University of Jerusalem Federmann Cyber Security Research Center.

2 *Statement: ICRC cyber-attack: Sharing our analysis*, ICRC (Feb. 16, 2022) https://www.icrc.org/en/document/icrc-cyber-attack-analysis [hereinafter: ICRC Cyberattack Statement]

work purposes.[3] Those impacted by the attack included "missing people and their families, detainees and others receiving services from the Red Cross and Red Crescent Movement as a result of armed conflict, natural disasters, or migration."[4] Once inside the system the hackers installed web shells to carry out "post-exploitation activities," which included among other things "compromising administrator credentials, moving throughout the network, and exfiltrating registry and domain files."[5] Following the incident the ICRC launched a campaign to notify victims of the data breach by the use of "phone calls, hotlines, public announcements, letters and in some cases in-person visits to remote communities."[6]

The cyber attack on the ICRC's servers highlights the importance of implementing and enforcing data protection and cybersecurity standards in the work of international organizations (IOs). These entities engage in a wide variety of data collection and processing work, that is only likely to increase in scope and volume in the years to come, and which includes personally indefinable information and confidential and sensitive materials. As Buchan and Tsagourias noted, "maintaining the confidentiality of this information is critical to enabling the IO to discharge its tasks and achieve its objectives."[7] This is especially true in the context of humanitarian action where "poor information management may spark violence and discrimination… may lead to stigma and ultimately threaten the actors' reputation, putting both employees and beneficiaries at risk."[8]

As this chapter will discuss, while some IOs have developed and put in place data protection frameworks, the practice is far from uniform. Even more troubling, the IOs that have introduced such frameworks have not done so out of a sense of an international legal obligation. Rather, data protection is introduced as a best practice or out of market or reputational demands. This chapter will explain why such a construction is

3 Carly Page, Red Cross says "state-sponsored" hackers exploited unpatched vulnerability, Tech Crunch (Feb. 16, 2022), https://techcrunch.com/2022/02/16/red-cross-links-january-cyberattack-to-state-sponsored-hackers/.

4 *See* ICRC Cyberattack Statement, *supra* note 2.

5 *See* Page, *supra* note 3.

6 *See* ICRC Cyberattack Statement, *supra* note 2. *See also* ICRC RULES ON PERSONAL DATA PROTECTION, Art. 20: Data Breaches (updated and adopted by the ICRC Assembly on Dec. 19, 2019) ("(1) Any breach of security leading to the accidental or unlawful destruction, loss or alteration of — or to the unauthorized disclosure of, or access to — Personal Data transmitted, stored or otherwise processed must always be reported to the ICRC Data Protection Office; (2) The persons affected must be notified of a Data Breach by the Staff in Charge, in close coordination with the Data Protection Office, without undue delay when the Data Breach puts them at particularly serious risk…") [hereinafter: ICRC RPDP].

7 Russell Buchan and Nicholas Tsagourias, *Hacking International Organizations: The Role of Privileges and Immunities*, ARTICLES OF WAR (Dec. 14, 2021), https://lieber.westpoint.edu/hacking-international-organizations-privileges-immunities/.

8 Theodora Gazi, *Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR*, 5 J. INT'L HUMANITARIAN ACTION 1 (2020),

problematic for the further development of international data protection law applicable in both war and peace.

While this chapter focuses on the ICRC as a case study, its arguments extend beyond this important organization. The past two decades have seen a large number of IOs voluntarily adopting data protection regimes, frameworks, and statements, including: The UN International Organization for Migration (IOM),[9] the UN Office of the High Commissioner for Refugees (UNHCR),[10] the UN World Food Programme (WFP),[11] the United Nations Office for the Coordination of Humanitarian Affairs (OCHA),[12] Oxfam,[13] and Médecins Sans Frontières (MSF).[14] While these organizations should be commended for their pioneering data protection work, all of them have failed to explicitly opine on whether international law constrains their data collection and processing practices. As a result, legal ambiguity remains as to the extent to which the practices of these IOs are sufficient, by themselves, to generate customary norms and expectations of behavior that could govern the actions of other IOs and non-State actors.

This brief chapter follows a two-part structure. Part I focuses on the needs for data protection frameworks in the work of humanitarian actors and further highlights the core framework that governs the data processing work of the ICRC. Part II shifts the discussion to the challenge

9 IOM was "one of the first international organizations to develop its own internal guidance concerning data protection, the IOM Data Protection Principles in 2009." *See* Data Protection, IOM, https://www.iom.int/data-protection. In 2010 the IOM released an even broader articulation of its data protection standards as part of the IOM Data Protection Manual (2010). The IOM was further a member of the UN Privacy Policy Group (UN PPG), which released the UN Principles on Personal Data Protection and Privacy. These principles were adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018. The principles bind all members of the UN system and represent a high-level framework for the processing of personal data.

10 *See* UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR (May, 2015), https://www.refworld.org/pdfid/55643c1d4.pdf; See also, UNHCR Guidance on the Protection of Personal Data of Persons of Concern to UNHCR (Aug. 2018), https://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=5b360f4d4. Since producing these two overarching documents, the UNHCR has been one of the most prolific in generating specialized data protection principles to address key aspects of its work. For example, consider the UNHCR Procedural Standards for Refugee Status Determination under UNHCR's Mandate (Aug. 2020), https://www.unhcr.org/4317223c9.pdf.

11 *See* WFP Guide to Personal Data Protection and Privacy: Principles and operational standards for the protection of beneficiaries' personal data in WFP's programming (June, 2016), https://docs.wfp.org/api/documents/e8d24e70cc11448383495caca154cb97/download/.

12 *See* OCHA Center for Humanitarian Data, OCHA Data Responsibility Guidelines (Oct. 2021), https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/60050608-0095-4c11-86cd-0a1fc5c29fd9/download/ocha-data-responsibility-guidelines_2021.pdf.

13 *See Responsible Program Data Policy* (Feb. 17, 2015), https://oxfamilibrary.openrepository.com/bitstream/handle/10546/575950/ml-oxfam-responsible-program-data-policy-en-270815.pdf;jsessionid=A1F3301F89806B21BA1F5EB6F708DFAE?sequence=1.

14 *See MSF Privacy and Personal Data Protection policy* (Jan. 22, 2019), https://msfaccess.org/privacy-and-personal-data-protection-policy.

of holding IOs accountable for potential privacy and data protection violations. This part explores both the general challenge of holding non-State actors responsible for protecting and ensuring human rights law, and the more specific concern in applying data protection rules as a matter of a customary international legal obligation applicable to IOs. The chapter concludes by briefly discussing the importance of recognizing data protection as an international legal obligation. This conclusion therefore recommends that all IOs adopt data protection frameworks and that they explicitly state that they have done so out of a sense of a binding international legal rule.

I
DATA PROTECTION IN HUMANITARIAN ACTION AND AT THE ICRC

The International Red Cross and Red Crescent Movement brings together the ICRC and 192 National Red Cross and Red Crescent Societies as well as their International Federation. As the largest humanitarian network in the world, it has a global reach. The ICRC alone has 20,000 staff working in over 100 countries.[15] The organization's work is based on the Geneva Conventions of 1949 and their Additional Protocols of 1977 as well as on the Movement's statutes and the resolutions of the International Conferences of the Red Cross and Red Crescent. Its core mandate is to ensure "humanitarian protection and assistance for victims of armed conflict and other situations of violence" by promoting "respect for international humanitarian law and its implementation in national law."[16]

To achieve this mandate in the digital age the ICRC relies on extensive data collection, processing, storage, and dissemination. As Figure 1 demonstrates, this is prevalent across every aspect of the work undertaken by the ICRC and its sister societies: from the use of data analytics and artificial intelligence to predict emergencies and allocate resources for disaster relief, through the use of cash transfer programs and biometrics collection in the management of facilities for refugees and asylum-seekers, all the way to the use of drones and social media applications in

15 *See* ICRC, *The International Red Cross and Red Crescent Movement*, https://www.icrc.org/en/who-we-are/movement.
16 *See* ICRC, *Mandte and Mission*, https://www.icrc.org/en/who-we-are/mandate.

Figure 1. Use Cases for Humanitarian Data Processing. Source: HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION 16-17 (C. Kuner & M. Marelli eds., 2nd ed., 2020).

the collection of evidence of abuses of rules of international humanitarian law (IHL).

The 37th International Conference of Data Protection and Privacy Commissioners, which convened in Amsterdam in 2015, adopted a resolution on privacy and international humanitarian action. In their Explanatory Statement the Commissioners described the increased need for both data in humanitarian action and rules to protect it:

> Identifying people and personal data processing are an integral part of the performance of the mission of humanitarian actors. The introduction of technology increases the number, nature and flow of data collected. In particular, this data is used to improve knowledge of beneficiaries, strengthen the effectiveness of humanitarian action and be accountable to beneficiaries. This trend may be beneficial if properly framed through privacy and data protection guarantees. However, if not properly framed, it could jeopardize human rights protection…
>
> Specific privacy and security risks are identified, including the potential for development of monitoring systems, which could

> be increased by technologies such as management information systems and electronic transfers; digital identity registration and biometrics, mobile phones but also drones. Humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally.

Strong data protection regimes and protocols will thus often complement and reinforce humanitarian action. On occasion, however, there may be "instances of friction" between the two. In such cases IOs will need to rely on "specific working procedures" to "justify derogations from the principles and rights" recognized under personal data processing regimes.[17] In other words, data protection frameworks should be seen as checks on IOs' effective execution of their mandates. When an IO introduces a new data-intensive practice into its sphere of operations, such practice should not result in counterproductive situations or undue risk of digital abuse or physical harm. After all, humanitarian actors are expected to follow the "do no harm" principle and to endeavor not to cause any further damage or suffering as a result of their activities.[18]

Against this backdrop it is perhaps surprising to learn that the ICRC only recently incorporated data protection norms and standards throughout the organization. The ICRC's Rules on Personal Data Protection (hereinafter: RPDP) were adopted in 2015 and, at the time, were one of the first comprehensive sets of data protection rules ever developed by a large humanitarian organization. The framework was meant to enable the ICRC "to remain at the forefront of international humanitarian action."[19]

The framework itself echoes and mirrors parallel regional and international data protection regimes. It generates a set of institutions within the ICRC with authority and capacity to ensure effective implementation

17 *See* HANDBOOK ON DATA PROTECTION IN HUMANITARIAN ACTION 29 (C. Kuner & M. Marelli eds., 2nd ed., 2020) [hereinafter: DATA PROTECTION HANDBOOK].

18 *See generally*, Jean Martial Bonis Charancle & Elena Lucchi, *Incorporating the Principle of "Do No Harm": How to Take Action Without Causing Harm: Reflections on a Review of Humanity & Inclusion's Practices* (Oct. 1, 2018), https://www.alnap.org/system/files/content/resource/files/main/donoharm_pe07_synthesis.pdf.

19 *See* ICRC RPDP, *supra* note 6, at 2.

(including a Data Protection Office and a Data Protection Commission).[20] It further establishes a set of principles to be followed by the ICRC in the conduct of its work:

1. Lawful, Fair, and Transparent Processing.[21]
2. Requirements for Specification and Minimization of Data.[22]
3. Requirements for Adequate and Relevant Data Storage.[23]
4. End-to-End Safeguards around Retention, Deletion, and Archiving.[24]
5. Data Subject Rights to Information, Access, Correction, Objection, Deletion, and in the context of Profiling.[25]
6. Data Protection Impact Assessments and Documentation Requirements.[26]
7. Specialized Rules for Data Breaches, Data Security, and Data Transfers.[27]

Within the limits of this chapter, I am unable provide a detailed account of this framework. Overall, however, the rules are designed "to reduce the risk of unauthorized use or access to personal data" by requiring the ICRC to follow "a 'data protection by design' approach."[28] Such an approach seeks "to minimize the collection of personal data to that which is necessary for the operation and ensure that data subjects' rights are respected."[29]

20 *Id.*, at 25-27 (Articles 26-28).
21 *Id.*, at 5-6 (Articles 1-2).
22 *Id.*, at 6 (Article 3).
23 *Id.*, at 7 (Articles 4-5).
24 *Id.*, at 8 (Article 6).
25 *Id.*, at 11-15 (Articles 7-14).
26 *Id.*, at 18 (Articles 17-18).
27 *Id.*, at 19-23 (Articles 20-25).
28 *Q&A: Humanitarian operations, the spread of harmful information and data protection: In conversation with Delphine van Solinge, the ICRC's Protection Advisor on Digital Risks for Populations in Armed Conflict, and Massimo Marelli, Head of the ICRC's Data Protection Office*, 102 Int'l Rev. Red Cross 27, 34 (2020).
29 *Id.*

II
THE CHALLENGE OF HOLDING IOS ACCOUNTABLE FOR DATA PROTECTION VIOLATIONS

In 2018 the Brussels Privacy Hub and the Data Protection Office of the ICRC joined forces to produce a "Handbook on Data Protection in Humanitarian Action." The handbook, now in its second edition, was produced with the desire to serve as a "useful tool to raise awareness and assist humanitarian organizations in complying with personal data protection standards."[30] The handbook was "inspired by a wide variety of data protection instruments"[31]—including the RPDP—"without being based solely on any single one of them."[32]

The handbook was explicit in suggesting that IOs are shielded from any meaningful domestic obligations concerning data protection. In the view of the editors, IOs "enjoy privileges and immunities to ensure they can perform the mandate attributed to them by the international community under international law in full independence and are not covered by the jurisdiction of the countries in which they work. They can therefore process Personal Data according to their own rules, subject to the internal monitoring and enforcement of their own compliance systems; in this regard they constitute their own 'jurisdiction'."[33]

The ICRC therefore does not consider itself bound by any domestic legal obligation to employ data protection standards. Any norms internalized are voluntary, non-binding, and reflective of "recognized best practices."[34] The ICRC further invites other international humanitarian organizations to follow this interpretive guidance. The ICRC therefore strongly believes that IOs' privileges and immunities should trump any external accountability or legal enforcement. Article 19 of the RPDP is in fact clear about that. While it does not preclude the possibility of cooperation with national or regional data protection authorities (DPAs), the Article simultaneously affirms that the ICRC "cannot be compelled to

30 Data Protection Handbook, *supra* note 17, at 11.
31 Christoper Kuner & Massimo Marelli, *Creating International Frameworks for Data Protection: The ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian action*, EJIL: Talk! (July 13, 2017), https://www.ejiltalk.org/creating-international-frameworks-for-data-protection-the-icrcbrussels-privacy-hub-handbook-on-data-protection-in-humanitarian-action/.
32 *Id*.
33 Data Protection Handbook, *supra* note 17, at 35.
34 *Id*.

disclose any information acquired while carrying out its work."[35] Instead of relying on external bodies like DPAs or local courts, the ICRC created the Data Protection Commission as the authority responsible to interpret the RPDP and to render decisions about their implementation, in particular in the context of arbitrating complaints by data subjects.[36]

It should be noted that the question of the applicability to IOs of domestic and regional data protection regimes, like the European General Data Protection Regulation (GDPR), is far from settled. "There is little precedent dealing with whether EU data protection law can apply to IOs" as these questions have "not arisen often in practice."[37] At least some scholars take the position that the application of these regimes to IOs "cannot be automatically excluded."[38]

Even assuming *arguendo* that IOs' privileges and immunities supersede any domestic application of data protection rules, such exclusion does not extend to international obligations. This is a crucial point so far ignored in prior discourse. All of the IOs who have produced internal data protection regimes have so far failed to address two crucial questions: (1) To what extent does data protection constitute a human right that is reflective of customary international law; (2) assuming that it is, could the obligations derived from that right extend to non-State actors, such as IOs.

Both of these points are highly controversial. As I have written elsewhere:

> Differences in legal cultures and perceptions mean there is still a lack of international consensus about basic questions of privacy and data protection, and there is still considerable fragmentation concerning core principles that govern this space. As such there is difficulty to verify the existence of any one principle as reflective of custom as a matter of "general practice accepted as law" under Article 38(1)(B) of the ICJ Statute.[39]

In other words, it is at least an ongoing question whether we can even articulate the right to data protection as a customary human right of relevance for our analysis. That said, it is certainly a possibility that over

35 *See* ICRC RPDP, *supra* note 6, at 18 (Article 19).
36 *Id.*, at 27 (Article 28).
37 Christopher Kuner, *International Organizations and the EU General Data Protection Regulation*, 16 Int'l Org. L. Rev. 158, 187 (2019).
38 *Id.*, at 188.
39 Asaf Lubin, *The Rights to Privacy and Data Protection under IHL and HRL*, in Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives 463, 475 (Robert Kolb, Gloria Gaggioli, & Pavle Kilibarda eds., 2022).

time the obligation could crystallize as more and more nations adopt data protection as a mandatory legal framework. Let us therefore proceed for the sake of argument with the assumption that the right to data protection is, or might become in the future, a right of customary character.

Even then, there will be a set of challenges applying the right to the ICRC as an IO. International human rights law (IHRL) generally places primary obligations on States. IOs "are rarely formal parties to human rights treaties, which usually address states and are drafted with the characteristics of states in mind."[40] Surely UN organs, which are bound by the Charter might be required to comply with human rights obligations as they are derived from the Charter.[41] Other human rights obligations might be considered *jus cogens* and therefore binding on all IOs. Data protection as a right, however, does not seem to be a good contender for a *jus cogens* status. Nor can data protection meaningfully be described as an obligation neatly derived from the general and vague commitments to human rights enshrined under the Charter.

More progressive interpretations of the human rights obligations of IOs do exist. These interpretations cite to "evolving practice in the Security Council and in the reports of some special rapporteurs"[42] which "increasingly consider that under certain circumstances non-State actors can also be bound by international human rights law and can assume, voluntarily or not, obligations to respect, protect, and fulfil human rights."[43] In any event, the point of this brief discussion is only to demonstrate the doctrinal complexity of trying to rely on international law, namely on customary rules of IHRL, to further cement the obligations of IOs to proactively produce and effectively enforce data protection standards in both peacetime and in war.

As a matter of future and evolving law there can be no question that a better articulation of IOs customary obligations, particularly in the data protection space, is of increasing importance. IOs now play a core function in our cotemporary world order. These organizations "effectively reflect transnational concerns and in turn strengthen the sense of global, human interdependence… creating an alternative world, one that

40 Gerald L. Neuman, *International Organizations and Human rights – The need for Substance*, Harvard Law School Human Rights Program Research Working Paper Series, (Apr. 2019), http://hrp.law.harvard.edu/wp-content/uploads/2019/04/Gerald-Neuman_HRP-19_001.pdf.

41 The preamble to the UN Charter speaks of "fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small." Article 1(3) similarly speaks of international cooperation "promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion."

42 UN Office of the High Commissioner for Human Rights, International Legal Protection of Human Rights in Armed Conflict 24 (2011).

43 *Id*.

is not identical with the sum of sovereign states and nations."[44] From a normative perspective surely international law should be imbued with the power to prevent gaps in legal coverage generated by the growth in scope and size of IOs. After all, States should not be allowed to create IOs to do their bidding which are then free from customary law or human rights obligations. In this regard there seems to be signs that courts are prepared to apply custom to non-State actors as a *general* international law that is sufficiently comprehensive to bind all actors on the international plane (although they may not be subject to the full gamut of legal rights and duties applicable to States).[45] This trend of expanding the reach of international custom to cover IOs should extend, where possible and relevant, to the areas of digital rights, informational privacy, data protection, and cybersecurity.

CONCLUSION: A CALL TO RECOGNIZE DATA PROTECTION AS AN INTERNATIONAL OBLIGATION ON IOS

At least one commentator has suggested that as IOs' data protection policies "become more widely adopted, they may lead to the gradual crystallization of international law."[46] This position would be true only if IOs adopted these data protection standards out of a sense of an international legal obligation. IOs, however, have so far treated data protection merely as a non-binding best practice.

44 Akira Iriye, Global Community: The Role of International Organizations in the Making of the Contemporary World 7 (2002).

45 *See e.g. Nevsun Resources Ltd v Araya* [2020] Supreme Court of Canada 5, para 107 (noting that "international law has so fully expanded beyond its Grotian origins that there is no longer any tenable basis for restricting the application of customary international law to relations between States."); *Reparations for Injuries in the Service of the United Nations*, Advisory Opinion, ICJ Rep. (1949) 174, 178 (noting that "the subjects of law in any legal system are not necessarily identical in their nature or in the extent of their rights, and their nature depends on the needs of the community."). For a broader reading see Robert McCorquodale, *An Inclusive International Legal System*, 17 Leiden J. Int'l L. 477 (2004).

46 Christopher Kuner, *The Internet and the Global Reach of EU Law*, *in* EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law 112, 131 (Marise Cremona & Joanne Scott eds., 2019) (referring in the immediate footnote that follows specifically to the possibility of crystallization of customary norms).

This book centers around the proposition that countries need to develop more robust international data protection legal regimes for wartime. Yet, if the ICRC—the primary IO whose mandate it is to promote respect for IHL—is unable to publicly declare that data protection is a customary human right of global enforcement, why should we ever expect States to do so?

United Nations organs and the ICRC are role models and are expected to lead by example. They set the tone that could ultimately usher in the progressive development of the law in the direction of enhanced digital rights and humanitarian protection of data. It is simply not enough therefore for the ICRC, and for parallel organizations, to merely "talk the talk" of data protection by adopting internal rules that they fully control and enforce without any sense of an external legal obligation to do so.

The growth of the datasphere generates new opportunities and complex legal and ethical challenges for the management of digital humanitarian spaces. For data protection regimes to offer an effective compass in traversing this new legal terrain, their role as a binding compass must first be recognized. The ICRC and other IOs must play their part in advancing the new agenda for wartime data protection by reaffirming their own legal commitments and obligations to the evolving international rule of law controlling in this area.

Digital Rights in the *Jus Post Bellum*

Chapter 13

The Investigation of Grave Crimes: Digital Evidence, the Right to Privacy, and International Criminal Procedure

Kristina Hellwig[1]

INTRODUCTION

International criminal courts and tribunals (ICTs) have been entrusted with the crucial but demanding task of prosecuting the most serious crimes in the fight against impunity. Technology has the potential to support this endeavor by providing valuable information. Since digital devices and new technologies have become integral parts of military operations and everyday civilian life, there is an ever-growing amount of digital data[2] with evidentiary value.[3] Therefore, digital evidence,[4] such as sat-

1 Lecturer, Hamburg University, Germany.
2 Hereinafter "data."
3 *See, e.g.*, Lindsay Freeman, *Law in Conflict: The Technological Transformation of War and Its Consequences for the International Criminal Court*, 51 N.Y. UNIV. J. INT. LAW POLITICS, 808, 860–61 (May 2019); Sean E. Goodison, Robert C. Davis & Brian A. Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, http://www.rand.org/pubs/research_reports/RR890.html (last visited Nov. 29, 2021).
4 A commonly used definition is that "[e]lectronic evidence is any data resulting from the output

ellite imagery, communication data, drone footage, and user-generated content (such as videos and photography), is becoming an essential tool in the fact-finding process.[5]

Interestingly, the use of such evidence is not entirely new. For example, at the International Criminal Tribunal for the Former Yugoslavia (ICTY), the Prosecution introduced aerial images provided by the U.S. military as evidence for the Srebrenica massacre.[6] Similarly, the introduction of videos, photographs, and other types of digital evidence is becoming common before the International Criminal Court (ICC) as well.[7] Recently, the ICC's Prosecution presented videos originally shared on social media, allegedly showing executions carried out by Mahmoud al-Werfalli[8] to prove its case. The Special Tribunal for Lebanon's Prosecutor also made use of video footage, special algorithms, and telecommunication data to determine the parameters of an explosion and connected actors in the *Ayyash* case.[9]

With the prevalence of new technologies and current developments in the fact-finding community, this trend will continue, and the role of digital evidence will likely increase. As technology develops, so does the way States and armed groups operate, especially in times of war. They utilize advanced technologies for law enforcement, military, and intelligence purposes,[10] thus producing large amounts of data with evidentiary value.[11] Given recent breakthroughs in robotics, machine learning, AI, and autonomous weapons, this development is unlikely to change.[12] Additionally, as social platforms and the World Wide Web are also utilized

of an analogue device and/or a digital device of potential [probative] value that are generated, processed, stored or transmitted using any electronic device. [And] [d]igital evidence is that electronic evidence that is generated or converted to a numerical format." *See, e.g.*, European Commission, *European Evidence Project, European Data Informatics Exchange Framework for Courts and Evidence*, http://www.cordis.europa.eu/project/id/608185/reporting/de (last visited Nov. 29, 2021); Maria A. Biasiotti et al., *Introduction: Opportunities and Challenges for Electronic Evidence, in* HANDLING AND EXCHANGING ELECTRONIC EVIDENCE ACROSS EUROPE, 3, 4 (Maria A. Biasiotti et al. eds., 2018). For a different proposal, see, for example, Burkhard Schafer & Stephen Mason, *The Characteristics of Electronic Evidence, in* ELECTRONIC EVIDENCE, 18, 19 (Daniel Seng & Stephen Mason eds., 4th ed. 2017). For an analysis of the characteristics of digital evidence, see Kristina Hellwig, *The Potential and the Challenges of Digital Evidence in International Criminal Proceedings*, INT. CRIM. L. R. (Advanced Articles 2021).

5 For an analysis of the evolution of digital evidence in ICL, see, for example, Lindsay Freeman, *Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials*, 41 FORDH. INT. L. J. 283, 291–307 (2018).

6 Prosecutor v. Krstić, IT-98-33-T, Judgment, ¶¶ 114, 223, 229 et seq., 250 (ICTY Aug. 2, 2001); Prosecutor v. Popović et al., IT-05-88-T, Judgment, ¶¶ 73–75 (ICTY June 10, 2010).

7 *See, e.g.*, Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2842, Judgment pursuant to Article 74 of the Statute, ¶ 93 (Mar. 14, 2012).

8 Prosecutor v. Al-Werfalli, ICC-01/11-01/17, Public Warrant of Arrest, ¶¶ 11–22 (Aug. 15, 2017) [hereinafter Al-Werfalli].

9 Prosecutor v. Ayyash et al, STL-11-01/T/TC, Judgment, at 107–11, 512–86, 605–39 (Aug. 18, 2020).

10 *See generally* Simone M. Friis, *"Beyond Anything We Have Ever Seen": Beheading Videos and the Visibility of Violence in the War against ISIS*, 91 INT. AFF. 725 (July 2015).

11 For more details, see, for example, Freeman, *supra* note 3; Goodison et al., *supra* note 3.

12 *E.g.*, Warren Chin, *Technology, War and the State: Past, Present and Future*, 95 INT. AFF. 765, 772 et seq. (July 2019); Freeman, *supra* note 3, at 813.

by some armed groups and States to spread propaganda, radicalize, or broadcast atrocities,[13] evidence of these actions exists in a digital format. For instance, ISIS uploaded videos showing beheadings,[14] which could serve as evidence in future trials, as is already evident by the social-media-derived evidence that has been introduced in *Al-Werfalli*.[15]

The growing importance of digital evidence is also spurred by civil society and NGOs. The fact-finding community has taken advantage of current technological developments within their documentation efforts,[16] allowing for an increase in third-party involvement[17] and open-source investigation.[18] Various activities, such as collecting, securing, analyzing, cataloging, and publishing large amounts of data on core crimes,[19] are carried out by NGOs, particularly for the purpose of enabling future criminal proceedings.[20]

Given the increase in digital information and its use as evidence, as well as the sheer volume of information being collected by various actors, the question arises as to what role the right to privacy plays in the investigation of core crimes and before ICTs in general. Thus, this chapter will attempt to provide an inventory of the right to privacy in international criminal procedure (ICP) with special regard to digital evidence and will address the role of ICTs in the protection of this right. While this topic is of paramount importance to all criminal tribunals dealing with core crimes, this inquiry will focus primarily on the ICC and use its procedural

13 *See, e.g.*, Freeman, *supra* note 3, at 833–34; *see generally*, Friis, *supra* note 10.
14 *E.g.*, Freeman, *supra* note 3, at 834; Friis, *supra* note 10.
15 Al-Werfalli, *supra* note 8, ¶¶ 11–22.
16 *E.g.*, Susann Aboueldahab & Inês Freixo, *App-Generated Evidence: A Promising Tool for International Criminal Justice*, 21 INT'L CRIM. L.R., 505, 505 et seq. (2021); Rebecca J. Hamilton, *User-Generated Evidence*, 57 COLUM. J. TRANSNAT'L. L., 1 (2018); Dia Kayyali et al., *Digital Video Evidence, When Collected, Verified, Stored and Deployed Properly, Presents New Opportunities for Justice*, ICC Forum, http://www.iccforum.com/cyber-evidence#Kayyali (last visited Nov. 29, 2021); Brianne M. Leyh, *Changing Landscapes in Documentation Efforts: Civil Society Documentation of Serious Human Rights Violations*, 33(84) UTR. J. INT'L & EUR. L. 44, 49 (2017).
17 In this context, the term "third party" refers to investigations by parties who are not directly involved in the proceedings and have no obligation to investigate, e.g., civil society organizations and NGOs.
18 Human Rights Center, UC Berkeley School of Law & UN Office of the High Commissioner for Human Rights, Berkeley Protocol, HR/PUB/20/2 (Dec. 1, 2020).
19 *See generally* Kayyali et al., *supra* note 16.
20 *See, e.g.*, the projects WITNESS (https://www.witness.org/our-work/, last accessed Jan. 22, 2022: "We coordinate with local citizens and organizations, conduct on-the-ground trainings, and provide free online resources in multiple languages"), Eyewitness (https://www.eyewitness.global/our-work, last accessed Jan. 22, 2022: "EyeWitness develops close partnerships with frontline organisations which document human rights violations that can amount to core international crimes, and with public interest litigators bringing these cases to trial"; "EyeWitness approach is based on three pillars"; "First, the… app allows you to capture photos and video that are embedded with metadata…"; "Second, when you send footage to the eyeWitness server we create a trusted chain of custody"; "Third, eyeWitness ensures the captured information is processed for justice") or Benetech (https://www.benetech.org/lab/ethical-ai-to-promote-justice/, last accessed Jan. 22, 2022: "By applying machine learning and computer vision to these videos, we hope to help them assess human rights violations and promote accountability and the rule of law in Syria and conflict settings worldwide").

rules as a case study having only limited opportunity to address the procedural perspective of the mixed tribunals. This chapter is structured as follows. Part I will focus on potential interference with the right to privacy that may occur during the investigation of core crimes. Part II will address the scope and effect of the right to privacy in ICP in general, while Part III will focus on the application of the right to privacy within the different investigative stages, focusing on the specific ICP rules of the ICC. By way of conclusion, this chapter will examine the future role that privacy rights could and should play before ICTs.

I
COLLECTING DIGITAL EVIDENCE OF GRAVE CRIMES AND POTENTIAL INTERFERENCE WITH THE RIGHT TO PRIVACY

Before analyzing the approach of ICTs regarding the right to privacy, it is necessary to at least briefly visualize how the collection of evidence on grave crimes may interfere with this right. Given how digital evidence is created, collected, and shared, an almost infinite number of scenarios are conceivable that may raise questions of the applicability and interference with the right to privacy. Thus, a complete representation will not be feasible in this chapter. However, this part will attempt to provide a general and manageable structural breakdown of what are arguably the most central groups of interventions.

Generally, privacy issues may arise during the creation or the use and processing of data. For instance, interference may occur when drone footage is recorded, video surveillance takes place, or audiovisual material is created by witnesses. Furthermore, interference may take place during the collection, storage, or transfer and sharing of such data. Gaining access to the content of data does not always require accessing the physical storage medium. It can be obtained by seizing the medium or device it is stored on but also by remote access to the data. Remote access may include sharing it via the internet, viewing the data digitally, or gaining access to the system and copying it (e.g., by interception or malware).[21]

21 *See, e.g.*, Goodison et al., *supra* note 3, at 5–8; Kayyali et al., *supra* note 16.

Additionally, as data is not bound to a single medium, it can be copied and widely disseminated rapidly.[22] In all these steps, multiple actors might take different roles, leading to new types of privacy issues. Overall, the applicable rules and standards may differ depending on the context, e.g., whether the collection was conducted during armed conflict or in peacetime.[23]

From the perspective of ICTs, digital evidence can be created by witnesses, journalists, and victims present on-site (e.g., videos or photographs of attacks or killings, mass graves or destruction of buildings) or gathered by the investigating bodies (e.g., independent investigations by the Prosecution, open-source investigation, etc.). They can also be created, collected, and provided to ICTs by a cooperating entity (e.g., States or NGOs). Which party is carrying out the measures can play a role in the determination of who can and should primarily ensure privacy protection or how far such responsibilities reach.[24] If ICTs wish to access certain data, then from a (criminal) procedural perspective, they can seek to use coercive means, such as interception or search and seizure,[25] but they may also get the data by voluntary transfer, such as by an NGO or a specific individual.[26] In general, coercive investigative measures regularly involve a privacy interference that may or may not be lawful depending on the adherence to the applicable procedural rules and national and international human rights standards. And while the determination of the applicable law can be a source of heated debate even in this more common context, the situation with voluntary disclosures is even more ambiguous. It is submitted here that interference with the right to privacy may also occur in cases where no coercive or covert means are applied and information is provided voluntarily, such as by NGOs or individuals.[27] This follows above all from the fact that the party collecting and providing the data to ICTs and the one whose privacy is affected can be different and can have contrasting standpoints. In this context, it must be asked whether, despite the fact that interference is primarily caused by others, the acceptance and use of third-party generated data by ICTs may nonetheless perpetuate the intrusion upon privacy rights. It is thus worth exploring the extent to which ICTs should take privacy rights into account in the context of such

22 *See, e.g.*, Kayyali et al., *supra* note 16.
23 *See, e.g.*, O'Connell (ch. 1 of this collection).
24 *See* Part III.A.
25 However, for the execution of coercive means, the ICT may have to rely on State cooperation. *See* Part III.A.
26 *See* Part III.
27 *See* Part III.B and the conclusion.

voluntary transfers, and the extent to which they can and should safeguard the protection of privacy rights even outside the scope of their own immediate activities.

II
GENERAL APPLICABILITY OF THE RIGHT TO PRIVACY

The right to privacy is codified in various human rights instruments[28] with broadly analogous scopes of protection, and many national constitutions and criminal codes recognize the importance of this right.[29]

By contrast, there is a lack of general reference to and recognition of this right within the ICTs' legal frameworks. It is explicitly mentioned only in the context of the rights of victims and witnesses and confidential communications.[30] During the drafting process, an interim version of the Rome Statute referred to the right and contained a provision on searches and seizures.[31] Ultimately, however, this provision was not included in the final version.[32]

However, the absence of an explicit reference does not mean that the right to privacy is not applicable before ICTs. For the ICC, this follows from Article 21 of the Rome Statute,[33] according to which internationally recognized human rights are an integral part of the applicable law, including the right to privacy.[34] And while such a rule is missing in the legal frameworks of the ad hoc tribunals, there is a strong rationale for

28 ICCPR, Art. 17; AmCHR, Art. 11; UDHR, Art. 12; ECHR, Art. 8. While the AfCHR does not refer to this right, many African constitutions and statutes do. *See* George Edwards, *International Human Rights Law Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy*, 26 YALE J. INT'L L. 324, 401–5.

29 For a detailed overview, see, for example, Edwards, *supra* note 28, at 400–5.

30 *See, e.g.*, ICTY, Rules of procedure and evidence, adopted Feb. 11, 1994, last amended July 8, 2015 [hereinafter ICTY RPE], Rule 75(A); ICTR, Rules of procedure and evidence, adopted June 25, 1995, last amended May 13, 2015 [hereinafter ICTR RPE], Rule 75(A); Rome Statute of the International Criminal Court, July 17, 1998, UN Doc. A/CONF.183/9 [hereinafter Rome Statute], Art. 57(3)(c), 68(1).

31 For a detailed illustration of the different versions of this provision, see, for example, Edwards, *supra* note 28, at 350–52.

32 Edwards, *supra* note 28, at 352.

33 Rome Statute, *supra* note 30, art. 21(3).

34 *See, e.g.*, Prosecutor v. Bemba Gombo et al., ICC-01/05-01/13, Judgment on the appeals of Mr. Jean-Pierre Bemba Gombo, Mr. Aimé Kilolo Musamba, Mr. Jean-Jacques Mangenda Kabongo, Mr. Fidèle Babala Wandu, and Mr. Narcisse Arido against the decision of Trial Chamber VII entitled "Judgment pursuant to Article 74 of the Statute," ¶ 284 (Mar. 8, 2018) [hereinafter Bemba II].

its applicability.[35] Accordingly, the ad hoc tribunals stressed that the lack of an explicit reference did not limit the need to act in conformity with recognized human rights,[36] including the right to privacy.[37] To interpret the scope of human rights, ICTs have relied on human rights jurisprudence in the past.[38] At the same time, they emphasized that this jurisprudence is not binding and that the context of international criminal law (ICL) may call for an adaptation of that scope.[39] It has been argued that some departures from domestic standards can be justified, given the *sui generis* goals of ICTs, the complexity and atrocity of the crimes they process, and the innate weaknesses of these tribunals[40] and also that, as ICL deals with crimes often committed in armed conflicts, insisting on peacetime due process standards would be unrealistic.[41]

Accordingly, due to this at least partial divergence from international human rights jurisprudence,[42] it is necessary to further analyze the different areas in which the right to privacy can be of relevance before ICTs and how the courts and tribunals apply this right in practice.

35 Arguments brought forward were, e.g., the applicability of the rules on international organizations, including human rights, references to human rights by the UN SC in their context, and the rule of law. For further details, see, for example, Lorenzo Gradoni, *The Human Rights Dimension of International Criminal Procedure, in* INTERNATIONAL CRIMINAL PROCEDURE, 74, 81 (Göran Sluiter ed., 2013); Yvonne McDermott, *The Influence of International Human Rights Law on International Criminal Procedure, in* INTERNATIONAL CRIMINAL LAW IN CONTEXT, 281 (Philipp Kastner ed., 2018).

36 *See, e.g.*, Barayagwiza v. Prosecutor, ICTR-97-19-AR72, Decision, ¶ 40 (Nov. 3, 1999).

37 *See, e.g.*, Prosecutor v. Brdjanin, IT-99-36-T, Decision on the Defence "Objection to Intercept Evidence," ¶¶ 28–29 (ICTY Oct. 3, 2003) [hereinafter Brdjanin].

38 *See, e.g.*, Situation in the Democratic Republic of the Congo, ICC-01/04-135-tEN, Decision on the Prosecution's Application for Leave to Appeal the Chamber's Decision of 17 January 2006 on the Applications for Participation in the Proceedings of VPRS 1, VPRS 2, VPRS 3, VPRS 4, VPRS 5 and VPRS 6, ¶ 34–40 (Mar. 21, 2006).

39 *See, e.g.*, Prosecutor v. Tadić, IT-94-1, Decision on the Prosecutor's Motion Requesting Protective Measures for Victims and Witnesses, ¶¶ 27–31 (ICTY Aug. 10, 1995) [hereinafter Tadić].

40 Mirjan Damaška, *The Competing Visions of Fairness: The Basic Choice for International Criminal Tribunals*, 36 2 N.C. J. INT'L L. 365, 380 (2010); Brdjanin, *supra* note 37, ¶ 63(7)–(9).

41 *Cf.* DAVID LUBAN, *Human Rights Thinking and the Laws of War, in* JENS D. OHLIN (ED.), THEORETICAL BOUNDARIES OF ARMED CONFLICT AND HUMAN RIGHTS, 45, 68 (2016).

42 For an in-depth analysis, see Amal Alamunddin, *Collection of Evidence, in* PRINCIPLES OF EVIDENCE IN INTERNATIONAL CRIMINAL JUSTICE, 231, 286 et seq., 301 et seq. (Karim A. Khan et al. eds., 2010); KRIT ZEEGERS, INTERNATIONAL CRIMINAL TRIBUNALS AND HUMAN RIGHTS LAW, 180 et seq. (2016).

III
THE PROTECTION OF THE RIGHT TO PRIVACY DURING THE INVESTIGATION

To carry out this analysis on the privacy rights approach before ICTs, this part will primarily focus on the procedural rules of the ICC, with some references to and examples from the ad hoc tribunals. The idea here is that the principles embodied in these procedural rules and the resulting problems are transferable, at least in their broad outlines, to other tribunals.

A THE PROTECTION OF THE RIGHT TO PRIVACY DURING STATE COOPERATION

Within the model of ICP, most investigative activities that go beyond voluntary cooperation with ICTs are intended to be conducted by the States obligated to cooperate.[43] In principle, this means that the collection of (digital) evidence, to the extent that disclosure is not voluntary, should be carried out by the cooperating States after a request by the ICT. For the ICC, Article 93 of the Rome Statute names various investigative measures that can be requested of Member States, including the execution of search and seizures (Article 93(1)(h)) and any other type of assistance, such as modern investigative techniques (Article 93(1)(l)).[44]

This naturally raises the question of the extent to which ICTs can influence the way the measures are carried out and thus have an impact on the observance of the right to privacy in this process. Following the general approach within ICP, as States conduct the requested measures according to their national procedure,[45] they should be mainly responsible for the protection of human rights during the execution of these

43 Rome Statute, *supra* note 30, Art. 86; S.C. Res. 827, ¶ 4 U.N. Doc. S/RES/827 (May 25, 1993); Statute of the International Criminal Tribunal for the Former Yugoslavia, S.C. Res. 827 (May 25, 1993) [hereinafter ICTY Statute], art. 29(1); S.C. Res. 955, ¶ 2, U.N. Doc. S/RES/955 (Nov. 8, 1994); Statute of the International Tribunal for Rwanda, S.C. Res. 955 (Nov. 8, 1994) [hereinafter ICTR Statute], art. 28(1).

44 ZEEGERS, *supra* note 42, at 166–67; Claus Kress & Kimberly Prost, *Article 93: Other Forms of Cooperation*, *in* ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT, 2078, 2086 (Otto Triffterer & Kai Ambos eds., 3rd ed. 2016). *See also* Rule 39(iii) of ICTY RPE, *supra* note 30, and of ICTR RPE, *supra* note 30.

45 *E.g.*, Rome Statute, *supra* note 30, art. 96 (3), 99(1).

measures, including the right to privacy.[46] However, this approach has clear shortcomings and leads to gaps in protection.[47] These gaps will be summarized here in a cursory manner. Furthermore, while ICTs are not mainly responsible for the conduct of the measures, it is possible to identify some instances where, at a minimum, it would be possible for the ICC (and the ad hoc tribunals) to consider and review the adherence to the right to privacy.

1 *Request for Cooperation*

An initial review of the measure's potential interference and compatibility with privacy rights by ICTs and their bodies could take place during the request for cooperation. However, this is not explicitly provided for in the ICT's legal framework, and some safeguards envisaged in the international human rights law (IHRL) jurisprudence are not fully applied.

In general, the ICC's Code of Conduct for the Office of the Prosecutor states that the Prosecution should respect the human rights and fundamental freedoms recognized by international law in conformity with the Statute.[48] However, as there are no public records of the requests for assistance and this rule is of a rather general nature, it is unclear which considerations are to be made before the request and how extensive any written reasoning should be.[49]

Additionally, while some authors have argued in favor of the need for a judicial warrant,[50] the ICC has not applied this approach until now.[51] Rather, the ICC emphasized that the Prosecution has independent authority to make cooperation requests under Article 93(1) Rome Statute.[52] This issue was also discussed before the ad hoc tribunals, where the tribunals have generally rejected the need for a judicial warrant approach.[53]

In addition, while the procedure regarding the formulation of the request envisaged in Article 96(2) of the Rome Statute could be utilized to weigh the conflicting interests against each other, including the rights

46 *Cf.*, Edwards, *supra* note 28, at 352 et seq.
47 For a detailed analysis, see ZEEGERS, *supra* note 42, at 113–86; Edwards, *supra* note 28, at 357.
48 ICC, Code of Conduct for the Office of the Prosecutor, Chapter 1, ¶ 8(1) (Sep. 5, 2013).
49 *See also* ZEEGERS, *supra* note 42, at 169.
50 *See, e.g.*, KAREL DE MEESTER, THE INVESTIGATION PHASE IN INTERNATIONAL CRIMINAL PROCEDURE: IN SEARCH OF COMMON RULES, 518 et seq. (2014); GÖRAN K. SLUITER, INTERNATIONAL CRIMINAL ADJUDICATION AND THE COLLECTION OF EVIDENCE, 125–28 (2002).
51 *See, e.g.*, Prosecutor v. Kenyatta, ICC-01/09-02/11, Decision on Prosecution's applications for a finding of non-compliance pursuant to Article 87(7) and for an adjournment of the provisional trial date, ¶¶ 28, 33 (Mar. 31, 2014) [hereinafter Kenyatta]; ROBERT CRYER ET AL., AN INTRODUCTION TO INTERNATIONAL CRIMINAL LAW AND PROCEDURE, 533 (2014); ZEEGERS, *supra* note 42, at 167.
52 Kenyatta, *supra* note 51, ¶ 33.
53 *See in detail, e.g.*, MARK KLAMBERG, EVIDENCE IN INTERNATIONAL CRIMINAL TRIALS: CONFRONTING LEGAL GAPS AND THE RECONSTRUCTION OF DISPUTED EVENTS, 252 (2013); ZEEGERS, *supra* note 42, at 153 et seq.

of those affected, there is no guarantee that such a process will take place in every case. The primary purpose of the obligation to provide certain information and reasoning is to enable the State to act under its national procedure,[54] and the rights of individuals are not explicitly mentioned.[55] And while Articles 96(2)(d) and 99(1) of the Rome Statute would allow the Court to proscribe procedural requirements, this possibility is rarely used.[56] Therefore, some authors have rightly argued that the request for State cooperation lacks sufficient and effective safeguards for the right to privacy.[57]

2 *The Execution of the Request*

There is reason to doubt the assumption that all national procedures applicable during the execution of cooperation requests uphold human rights standards and thus provide sufficient protection.[58] Even those States whose procedural rules comply with human rights in general might diverge from them in the context of State cooperation in a manner incompatible with privacy rights.

According to Article 96 of the Rome Statute, the Court must provide information on the case and the reasons for the request, such as the legal grounds and the circumstances of the case. Hence, in a best-case scenario, the State would have sufficient information to assess the request's conformity with human rights.[59] In case of non-conformity, the State could reject the request, as Part 9 of the Rome Statute gives grounds for refusal such as conflicting treaty obligations[60] or incompatibility with existing fundamental legal principles of general application.[61] Both grounds could be used to refuse investigative means contrary to human rights standards.[62]

In many cases, however, the procedure for State cooperation with the ICC, which is often conducted in a manner similar to inter-State cooperation, does not provide sufficient safeguards that at the end of the process, one of the parties, either the requestion or the executing party, will verify that the measures are compatible with human rights.[63]

54 ZEEGERS, *supra* note 42, at 169 et seq.
55 *See also id.* at 169–70.
56 *Id.* at 170–71.
57 *Id.* at 171.
58 *Id.*
59 *Id.* at 173.
60 Rome Statute, *supra* note 30, art. 97(c).
61 *Id.* art. 93(3).
62 *See, e.g.*, Kenyatta, *supra* note 51, ¶ 37; Claus Kress & Bruce Broomhall, *Implementing Cooperation Duties under the Rome Statute: A Comparative Synthesis*, *in* THE ROME STATUTE AND DOMESTIC LEGAL ORDERS, VOL. II, 515, 531 (Claus Kress et al. eds., 2005); ZEEGERS, *supra* note 42, at 172.
63 ZEEGERS, *supra* note 42, at 174; CRYER ET AL., *supra* note 51, at 534.

As some authors rightly argue, without specific legislation, there is an increased risk that cooperative States trying to support ICTs will fail to sufficiently protect human rights.[64] If requested, they might be unwilling to perform a genuine test for political reasons or due to the strength of mutual trust.[65] As a result, some States are implementing the requests without any review or special procedure.[66] Hence, even though the Rome Statute provides grounds for refusal, States may not use these means in order to attend to their duty to cooperate.[67] In addition, the human rights situation in some cooperating States makes it inappropriate to rely on them to protect human rights.[68]

3 *Ex Post Review during the Evaluation of Evidence*

One remaining option is the *ex post* review of the compatibility of measures with human rights. The procedural rules on the admissibility of evidence require such an analysis to some extent, as evidence obtained by means violating internationally recognized human rights is inadmissible if the violation casts substantial doubt on its reliability or if the admission would be antithetical to and seriously damage the integrity of the proceedings.[69] This assessment requires a determination of first, whether the evidence was obtained illegally, and second, whether this violation is sufficient to render it inadmissible.[70]

An analysis of the jurisprudence shows a positive trend, especially in the context of the ICC, towards the increasing review of alleged violations of privacy rights within the investigative stage of proceedings. For instance, when confronted with allegations that evidence was obtained illegally and in violation of the right to privacy, the ICTY often reviewed the legality in only a limited manner.[71] A frequently chosen approach was to focus on the good faith of the investigators.[72] By contrast, the ICC has developed a more detailed review. While the ICC does not elaborate on the process's compatibility with national procedure,[73] it has reviewed compliance with the internationally recognized standard of protection

64 *E.g.*, ZEEGERS, *supra* note 42, at 173–74.
65 *Id.* at 173; Kress & Broomhall, *supra* note 62, at 526 et seq.
66 ZEEGERS, *supra* note 42, at 173; Kress & Broomhall, *supra* note 62, at 526 et seq.
67 ZEEGERS, *supra* note 42, at 172.
68 *See also id.* at 173–74.
69 *See, e.g.*, ICTY RPE, *supra* note 30, Rule 95; ICTR RPE, *supra* note 30, Rule 95; Rome Statute, *supra* note 30, art. 69(7).
70 *See, e.g.*, Bemba II, *supra* note 34, ¶ 280; Brdjanin, *supra* note 37, ¶¶ 57–68.
71 *See, e.g.*, Brdjanin, *supra* note 37, ¶¶ 57–60; Prosecutor v. Haraqija et al., IT-04-84-R77.4, Decision on Morina and Haraqija Second Request for a Declaration of Inadmissibility and Exclusion of Evidence, ¶ 19 et seq (Nov. 27, 2008) [hereinafter Haraqija].
72 *E.g.*, Brdjanin, *supra* note 37, ¶ 63(1); Haraqija, *supra* note 71, ¶ 19 et seq.
73 Rome Statute, *supra* note 30, art. 69(8).

for the right to privacy and in some cases decided that there was indeed a violation of these standards.[74] However, in *Mbarushimana*, the Chamber argued that the defense had failed to provide sufficient information on the illegality of the collection of evidence and that therefore there was no burden on the Prosecution to show that the evidence was not obtained in violation of the Statute or internationally recognized human rights.[75] The Chamber also noted that there is a presumption that the investigative activities were carried out in accordance with the provisions applicable in that State. This approach of shifting the burden of proof regarding the measures' incompatibility with the applicable law is problematic. It limits the scope and extent to which the ICC assesses and takes responsibility for the way investigative measures are conducted. Furthermore, this limiting interpretation of Article 69(7) of the Rome Statute and the divergence from IHRL (according to which the defense must merely prove the occurrence of an interference and not that this interference was unlawful, which from an IHRL perspective must be proven by the State) was made without providing sufficient rationale.[76] A preferable approach was taken later on by the Appeals Chamber in *Bemba II*, where the Chamber emphasized the need to determine whether an action was in accordance with internationally recognized human rights, including whether the interference was proportionate to legitimate investigative needs.[77] The proportionality determination must take the nature of the information and the sensitivity of such data into account, and these interests must be weighed against the pursued investigative need warranting the access.[78]

The extent to which illegally obtained evidence is admitted is also pertinent because declaring such evidence inadmissible could indirectly reinforce the right to privacy for future proceedings. ICTs have brought forward different lines of argumentation for the admissibility of evidence in privacy violation circumstances.[79] For instance, the ICTY has argued that neither international law nor (a relevant number of) national legal systems prescribe the automatic exclusion of illegally obtained evidence.[80] Furthermore, a Chamber has noted that, particularly in the context of

74 *E.g.*, Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06-803-tEN, Decision on the confirmation of charges, ¶ 81 (Jan. 29, 2007) [hereinafter Lubanga]. For instance, in *Lubanga*, the Chamber found that the search and seizure of hundreds of documents and items, including correspondences, photographs, diaries, and many more, was disproportionate.
75 Prosecutor v. Mbarushimana, ICC-01/04-01/10, Decision on the confirmation of charges, ¶ 60 (Dec. 16, 2011).
76 *See also* ZEEGERS, *supra* note 42, at 178.
77 Bemba II, *supra* note 34, ¶ 330 et seq.
78 *Id.* ¶ 333.
79 *See in detail, e.g.*, Alamunddin, *supra* note 42, at 296; Damaška, *supra* note 40, at 365–88.
80 Brdjanin, *supra* note 37, ¶ 31 et seq.

armed conflicts, intelligence can be essential in uncovering the truth.[81] It is also argued that, in light of the gravity and seriousness of the charges and the jurisdiction and purpose of the tribunals, even illegally intercepted evidence obtained in a pre-armed conflict period must be regarded as admissible.[82] The ICC has regularly come to the same conclusion and has not excluded evidence obtained in violation of privacy rights.[83] For instance, the ICC has argued that even though there is no consensus in international law, the majority is of the view that only serious human rights violations can lead to the exclusion of evidence.[84] Accordingly, since evidence is rarely excluded based on violations of the right to privacy, such an indirect influence is questionable.

B THE PROTECTION DURING INVESTIGATIONS BY THE ICT'S PROSECUTORS

Another area of importance is whether there are sufficient safeguards for the protection of privacy rights in the context of investigative activities by the Prosecution and the overall activities of ICTs.

1 *General*

It should first be emphasized that ICTs, and the ICC in particular, have very limited authority to implement coercive measures outside the context of State cooperation. Rather, search and seizures and interceptions are regarded as on-site investigative activities that depend on the cooperation of States or their approval.[85] While the ad hoc tribunals had limited independent investigative means,[86] the Rome Statute provides this possibility only in a very restricted manner.[87] The Prosecution can only conduct such independent on-site investigations in the context of Article 54, 57(3)(d) of the Rome Statute, that is, when a State is unable to execute a request for cooperation due to the unavailability of any authority or any component of its judicial system.

81 *Id.* ¶ 61.
82 *Id.* ¶ 63(8).
83 Bemba II, *supra* note 34, ¶ 44; Lubanga, *supra* note 74, ¶¶ 83–90.
84 Lubanga, *supra* note 74, ¶ 86.
85 *See, e.g.*, Alamunddin, *supra* note 42, at 258.
86 The ad hoc tribunals were provided with more extensive direct investigative rights. *See, e.g.*, ICTY Statute, *supra* note 43, art. 18(2); ICTR Statute, *supra* note 43, art. 17(2); Prosecutor v. Blaškić, IT-95-14-AR108 bis, Judgment on the Request of the Republic of Croatia for Review of the Decision of Trial Chamber II of 18 July 1997, ¶ 53 (Oct. 29, 1997); RICHARD MAY & MARIEKE WIERDA, INTERNATIONAL CRIMINAL EVIDENCE, 62, 67 (2002).
87 *See, e.g.*, MEESTER, *supra* note 50, at 516; ZEEGERS, *supra* note 42, at 147.

However, even aside from this area, it is relevant to consider what role the right to privacy may play in the Prosecutor's investigations. This is especially true given the increase in open-source investigation and data sharing by a wide variety of actors, even without what are known as coercive measures. Moreover, it should be noted that the voluntary disclosure of data to the Court does not necessarily mean that the data has been obtained in a way consistent with the right to privacy or that there has been no interference with it.[88] In addition, data protection and protection from third-party interference is especially important in the context of sensitive data that may be in the possession of ICTs.

To date, there has been only a very limited general policy in place that could sufficiently protect the right to privacy. While the ICC has developed an E-court Protocol[89] on digital evidence, this protocol does not refer to privacy rights but rather aims at standardizing technical-data-type-related questions. The ICC's Code of Conduct for the Office of the Prosecutor does state that the Office of Prosecution should respect the human rights and fundamental freedoms recognized by international law in conformity with the Statute.[90] Similarly, the Regulations of the Office of the Prosecution refer to the privacy in relation to confidential correspondence,[91] and Article 21(3) of the Rome Statute provides that the ICC is bound to respect internationally recognized human rights. However, as these provisions are of a very general nature, there is no certainty in how they are applied to privacy issues.

Therefore, it would be desirable for ICTs to develop specific standards for investigations performed by the ICTs bodies, especially in relation to the right to privacy.[92] These standards should find a balance between the investigative interests and the rights of those affected. They could address issues such as the protection of victims or potential witnesses visible in digital materials, or the outstanding issue of the types of data to be collected or the means of data collection, storage, and processing. While it would be desirable to include such standards in the Rules of Procedure and Evidence (RPE) of ICTs, as these new types of investigative methods will only increase in the future, this option could be difficult to achieve in practice. Nevertheless, official statements and policies could

88 *See also* Kayyali et al., *supra* note 16.
89 Unified Technical protocol for the provision of evidence, witness and victims' information in electronic form, ICC-01/14-01/18-64-Anx (Jan. 23, 2019).
90 Chapter 1, ¶ 8(1).
91 Reg. 21; Reg. 28(2).
92 *See also, e.g.*, Asaf Lubin, *The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law*, *in* Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives, 490–91 (Robert Kolb et al. eds., 2022).

provide some clarity on ICTs' approach regarding the right to privacy in the digital domain.

2 *The Special Protection of Victims and Witnesses*

As noted, the only explicit reference to the right to privacy within ICP can be found in the context of victims and witness protection and confidential correspondences. In the context of ICL, the protection and the privacy of victims and witnesses has a particularly important role. The dangers for them are not only of a theoretical nature and were already evident in the first years of the ad hoc tribunals. For instance, in the first years of the tribunal, some witnesses who testified before the International Criminal Tribunal for Rwanda (ICTR) were killed upon arriving back home.[93] Hence, the ad hoc tribunals attached particular importance to the protection of witnesses and victims.[94] Similarly, the ICC's legal framework entails rules on the protection of witnesses. According to Article 68(1) of the Rome Statute, the Court shall take appropriate measures to protect the safety and privacy of victims and witnesses. This general provision aims at placing on all organs of the Court the obligation to take appropriate measures.[95] In this regard, the Court must consider all relevant factors, including age, gender, and health, as well as the nature of the crimes.[96] Possible measures may be the prevention of releases to the public or the media on the identity or location of a victim, witness, or other person at risk.[97] Hence, witnesses are, in general, not named publicly and are known by pseudonyms in proceedings.[98]

This raises the question of what protection might look like in the context of modern technologies and digital evidence. So far, there is little experience to go on regarding the impact of the increased prevalence of digital evidence. It is important to bear in mind that audiovisual evidence in particular can show not only the perpetrators but also third parties, victims, and witnesses, and metadata and personal information can be used to identify individuals. Some have argued that the existence of audiovisual evidence could ensure the safety of witnesses and victims, as they are not the only ones providing incriminating proof.[99] However,

93 *See, e.g.*, David Donat-Cattin, *Art. 68*, *in* Rome Statute of the International Criminal Court: A commentary, 1681, 1683 (Otto Triffterer & Kai Ambos eds., 3rd ed. 2016).
94 *Id.*
95 *E.g.*, William Schabas, The International Criminal Court: A Commentary on the Rome Statute, 1058 (2016).
96 Schabas, *supra* note 95, at 1058.
97 *Id.*
98 *Id.*; *cf.* Tadić, *supra* note 39, ¶¶ 27–31.
99 *E.g.*, Keith Hiatt, *Open Source Evidence on Trial*, 125 Yale L. J. Forum 323, 325 (2016).

others have rightly expressed concerns regarding identifiability via digital evidence,[100] which could endanger parties not present before the ICTs. Especially in the early stages of investigations, where witnesses are still being sought, the prevalence of digital media could pose a threat to victims and witnesses. Moreover, during ongoing conflicts, the availability of information on informants, witnesses, and victims could be harmful to them. As practice shows, civilian populations are increasingly active in collecting evidence on grave crimes. NGOs and civil society in particular tend to use digital data for the collection.[101] Collections that do not sufficiently protect the privacy of the identifiable individuals could pose immeasurable threats to those on site.

The latter norms could be used to protect those affected. There are still some legal uncertainties, especially concerning whether the standards can be interpreted to apply to victims shown in digital and documentary evidence. While an overly broad interpretation of the above-mentioned provisions may make their fulfillment impossible, an overly narrow interpretation might harm those trying to support investigations. Hence this rule should generally also apply in the context of digital evidence; however, the interpretation and understanding of the appropriate means may vary in this context. Conceivable technical means here could be to make faces unrecognizable if they are not relevant for the proceedings and establish data collection in a manner that protects personal information that could be used to identify specific individuals. An additional safeguard would be to not share potential evidence publicly.

Overall, States and ICTs should seek to adopt approaches that do not pose additional harm to victims and witnesses, regardless of whether they testify in person or by providing documentary proof.

3 *Protection during Cooperation with NGOs and Civil Society*

As elaborated above, NGOs are engaging more and more in fact-finding or quasi-investigative functions, especially by using digital data. They collect information shared on social media or provided to them by individuals and create large data collections with considerable potential to support ICP. However, there are also risks involved, especially in relation to the protection of human rights. This follows above all from the fact that the party collecting and providing the data to ICTs and the one

100 *See, e.g.*, Beth van Schaack, *Fourth Industrial Revolution Comes to the Hague*, http://www.iccforum.com/cyber-evidence#Van-Schaack (last visited Nov. 29, 2021); Kayyali et al., *supra* note 16; Hiatt, *supra* note 99, at 324; Hamilton, *supra* note 16, at 60; Aboueldahab & Freixo, *supra* note 16, at 523.

101 *E.g.*, Hellwig, *supra* note 4.

whose privacy is affected can differ and that both can have contrasting standpoints. For example, while a portion of data is shared with ICTs by individuals willing to take the risks involved, other information is collected or shared without consent and, in some cases, by the perpetrators. Furthermore, if recordings and large data collections are openly accessible, they could be used to identify not only alleged perpetrators but also collectors, victims, and witnesses. This may significantly affect their right to privacy and sometimes also their safety, especially in ongoing conflicts. Therefore, the protection of potentially affected parties throughout the process is essential.[102]

However, there is a lack of internationally applicable law in this framework. Data collections today are rarely established and overseen by ICT's Prosecutions; instead, this is typically done by various NGOs. Within the current international legal framework, there are no clear internationally binding obligations for NGOs to respect human rights. While attention should be drawn to NGOs' efforts to develop voluntary standards on these issues, such as with the Berkeley Protocol,[103] precisely because of the voluntary nature of these instruments, there is still a pressing need to find additional safeguards. Furthermore, while these entities largely act independently, the acceptance and use of the data by ICTs may perpetuate interference in the affected individuals' right to privacy.

As a number of collections are aimed specifically at enabling criminal proceedings, ICTs are in a unique position to influence this sector towards a more privacy-conscious approach. Thus, while it may be difficult to argue that ICTs and other fact-finding bodies have an obligation to regulate this sector, they could take a more active role in safeguarding the protection of such rights even outside the scope of their own activities.

Therefore, the question arises of how to achieve higher standards in this area. As ICTs rarely exclude evidence based on privacy violations, it is unlikely that the threat of exclusion of the collected evidence alone could lead everyone to adhere to privacy regulations. Possible solutions include the implementation of additional (binding) guidelines[104] or contract relations with the ICT's Prosecutions[105] or other fact-finding bodies. The latter possibility in particular could help to realize the potential

102 *See also, e.g.*, Aboueldahab & Freixo, *supra* note 16, at 507, 521.
103 Berkeley Protocol, *supra* note 18.
104 *E.g.*, Elena A. Baylis, *Outsourcing Investigations*, 14 UCLA J. INT'L L. FOREIGN AFF. 121, 146 (2009); International Bar Association, *Evidence Matters in ICC Trials*, 26 (Aug. 2016); Alexander Heinze, *Private International Criminal Investigations*, Z. INT. STR. DOGM. 169, 181 (Feb. 2019).
105 Hamilton, *supra* note 16, at 53–61.

offered by these activities without excessive strain on the rights of the persons concerned if contracts would contain provisions on the respective rights to be protected.

CONCLUSION: WHAT IS THE ROLE OF ICTS IN THE PROTECTION OF THE RIGHT TO PRIVACY?

This chapter has provided an overview of the areas in which the right to privacy could be of relevance in ICP and where future issues may occur. It is not yet apparent if ICTs have sufficiently adapted to the increasing relevance of digital evidence. Overall, while the right to privacy is recognized in ICL, better approaches to enforcing this right are desirable. Two main areas for action can be identified.

First, standards and policies should be established for ICTs' own activities.[106] This would be beneficial in light of transparency concerns, existing responsibilities to witnesses and victims, and the commitment to human rights. In this context, there is a need to develop sufficient standards to protect victims and witnesses but also find a sufficient procedure for open-source investigation. It should be borne in mind that open-source investigations and voluntary disclosures of data are not completely free of potential interference with the rights of data subjects.[107]

Second, the role of the right to privacy in the context of cooperation must be reevaluated. In many ways, ICTs must deal with rather limited availability of evidence, and the crimes they deal with are of such seriousness that violations of the "mere" right to privacy do not take a prominent role. Therefore, some have argued that this right must yield second place to the interests of the victims seeking justice and the interests of the international community.[108] However, this line of argument is not fully convincing. While it is correct that ICTs do not have the function of disciplining national armies or authorities,[109] ICTs and national authorities are bound to respect international human rights. If commonly applied investigative procedures are incompatible with such rights, they must be

106 *See also, e.g.*, Lubin, *supra* note 92, at 490.
107 Kayyali et al., *supra* note 16.
108 Brdjanin, *supra* note 37, ¶ 63(7); Lubanga, *supra* note 74, ¶ 86.
109 Brdjanin, *supra* note 37, ¶ 63(9).

adjusted. In many cases, the issue is not so much whether the measures should be implemented at all but rather that procedural standards and safeguards must be complied with, or in some cases, developed in the first place. There needs to be a structural adjustment within the investigative process to ensure the predictability and monitorability of measures. For this reason, authors have rightly called for *ex ante* checks on the ordering of coercive measures ensuring compliance with the right to privacy.[110] *Ex post* checks are also crucial.[111]

Given the increasing relevance of the digital domain, limiting the scope of the right to privacy and the acceptance of an approach to ICP in which the imperative for human rights protection is outweighed by the need for evidence[112] is concerning. Upholding human rights standards, and not only to a minimum, conveys respect for human rights by demonstrating fairness and adherence to legal rules even in the context of prosecuting mass atrocities.[113] Omitting privacy rights could have an overall derogatory effect on the rights in question, as well as on the approval of ICTs by the international community and the acceptance of their rulings by local communities. This holds at least the risk that some entities question their legitimacy. In addition, privacy protection can also safeguard other human rights (e.g., the right to life and the right to freedom from arbitrary detention), especially in the context of ICP. Therefore, ICTs should take a more prominent role in promoting these rights and upholding human rights standards.

110 Zeegers, *supra* note 42, at 186.
111 *Id.*
112 Damaška, *supra* note 40, at 386.
113 *See generally* Yvonne McDermott, Fairness in International Criminal Trials (2013); Salvatore Zappalà, Human Rights in International Criminal Proceedings (2005).