A Comprehensive Analysis of Privacy and Data Protection in Conflict-Affected Areas: Revising Human Rights and Humanitarian Law to Address the Challenges of Surveillance Technologies

Utrecht University

Faculty of Law, Economics and Governance

Student Name: Masoumeh Rahimi

Student Number: 2843447

Supervised by: Dr. Alexandra Hofer

Master's Thesis in Public International Law (Conflict and Security Track)

Date of Completion: 27th June 2024

Word count:17465

Contents

Abbreviations

AI - Artificial Intelligence

AP- Additional Protocol

ECHR- European Convention on Human Rights

ECtHR - European Court of Human Rights

EU- European Union

FPV- First Person View drones

GC- Geneva Conventions

GDPR - General Data Protection Regulation

HR - Human Rights

IAC - International Armed Conflict

ICCPR - International Covenant on Civil and Political Rights

ICJ - International Court of Justice

ICRC - International Committee of the Red Cross

IHL - International Humanitarian Law

IHRL - International Human Rights Law

IO - International Organization

NATO- North Atlantic Treaty Organization

NGO - Non-Governmental Organization

NIAC- Non-International Armed Conflict

OECD- Organisation for Economic Cooperation and Development

UAV - Unmanned Aerial Vehicle

UDHR - Universal Declaration of Human Rights

UN - United Nations

UNGA - United Nations General Assembly

1 Introduction

In 2017, The Guardian reported that a Palestinian laborer was arrested after a mistranslated Facebook post was flagged by Israeli authorities, because they used surveillance to monitor Palestinians on social media.[1] This case highlights how civilians' data is monitored by authorities and how using new technologies poses challenges to protecting data and the right to privacy of them in occupation.[2]

The right to privacy is a human right that primarily addresses the protection of individuals from intrusion into their personal affairs and the non-interference of personal spheres.[3] To respect this right, individuals must have control over their personal information and freedom from unwarranted surveillance, physical searches, and interference in private matters.[4] This right can be restricted only for clear reasons, including national security, protection of public safety, or prevention of crimes; nevertheless, it is not allowed to be unlawful, unnecessary, or disproportionate.[5] The right to data protection is closely related to privacy, which ensures individuals have control over their personal data collection; however, this right has not been given a separate status of recognition in International Human Rights Law (IHRL).[6]

In the time of International Armed Conflicts (IACs) and occupation, the application of new technologies, specifically surveillance drones,[7] and data collection techniques[8] such as biometric technologies are remarkable ways to collect data that is functional in military operations and the establishment of public order in occupied areas.[9] Based on Common Article 2 of the Geneva Conventions (GCs), the term IACs is applied to conflicts between two or more states involving the use of armed forces, which are governed by International Humanitarian Law (IHL).[10] Furthermore, in accordance with the 1907 Hague Convention, the condition of occupation arises when a territory is effectively placed under the control of a foreign military force.[11]

The deployment of new technologies for collecting data in intelligence operations could potentially have benefits in line with the underlying principles of IHL, such as the principle of distinction; however, it is controversial because the collected data has been used for killings,

---

[1] Alex Hern, 'Facebook translates "good morning" into "attack them", leading to arrest' (The Guardian, 24 October 2017), <https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest >, accessed 10 April 2024.
[2] *Ibid.*
[3] Andrei Marmor, 'What Is the Right to Privacy?' (2015) 43 Phil & Pub Aff 3-26, 10-12.
[4] *Ibid*, 12.
[5] *Ibid*, 14.
[6] Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not So New Right' (2013) 3(2) Intl Data Privacy L 88-99, 90.
[7] Surveillance drones, also known as Unmanned Aerial Vehicles (UAVs).
[8] These techniques include technologies utilize unique physical or behavioural attributes of individuals for identification and authentication purposes.
[9] Christof Heyns, Dapo Akande, Lawrence Hill-Cawthorne, and Thompson Chengeta, 'The International Law Framework Regulating the Use of Armed Drones' (2016), 65(4) International & Comparative Law Quarterly 791-827, 791.
[10] Emily Crawford and Alison Pert, International Humanitarian Law (2nd ed, Cambridge University Press 2020), 55-57.
[11] *Ibid*, 160.

and making mistakes in targeting is possible.[12] For this reason, such operations have been the subject of detailed discussions at the United Nations (UN) and *jus ad bellum* levels to clarify their legality.[13] However, the impact of using such technologies for surveillance and the privacy of non-combatants, specifically civilians, has received little study until this date.[14]

The utilization of surveillance drones and biometric collection technologies creates concerns for civilians' privacy. In this regard, Harry Wingo, a cybersecurity expert, affirms that "surveillance drones raise privacy concerns because of their ability to harness powerful camera technology along with the ability to observe persons in ways that have been previously impossible."[15] The increase in the use of such technologies in recent conflicts has made civilians who live in conflict-affected areas feel that they are always being controlled, and this could deprive them of some other fundamental human rights such as the rights to freedom of movement and freedom of expression.[16] For instance, the New York Times reported in 2011 that a citizen in Afghanistan "would almost have to spend every minute in a home village and never seek government services to avoid ever crossing paths with a biometric system."[17]

The main legal framework that applies in the times of IACs and occupations is IHL.[18] Additionally, according to public international knowledge such as the *Wall Advisory Opinion*[19] and the *Nuclear Weapons Advisory Opinion* [20] of the International Court of Justice (ICJ), cases such as *Hassan v. United Kingdom*[21] before the European Court of Human Rights (ECtHR), and the doctrine of IHL, the IHRL continues to apply during armed conflicts alongside the IHL in cases regarding human rights.[22] Therefore, an armed conflict does not deprive people of their right to data privacy, and restricting this right must be limited to the legal conditions.

However, neither the IHL frameworks, including the Geneva Conventions (GC I-IV) nor the International Covenant on Civil and Political Rights of 1966 (ICCPR), have direct regulations on the impact of using such technologies in conflicts on civilian data protection and their right to privacy.[23] Given that these technologies did not exist at the time these conventions were drafted, another critical question is how existing rules apply to these new developments. This gap in the applicable legal frameworks leaves a serious space for violations against the right to privacy of civilians, which highlights a normative gap because there are no specific rules to

---

[12] Eliza Watt, 'The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (NATO CCDCOE Publications 2022), 157-180, 158.
[13] See Philip Alston (Special Rapporteur), 'Report on Extrajudicial, Summary or Arbitrary Executions' (2010) UN Doc A/HRC/14/24/Add.6, para 1.
[14] Watt (n 12), 158.
[15] Harry Wingo, 'Set Your Drones to Stun: Using Cyber-Secure Quadcopters to Disrupt Active Shooters' (2018), 17(2) Journal of Information Warfare 54-64, 59.
[16] Watt (n 12), 161-162.
[17] Thom Shanker, 'To Track Militants, US Has System That Never Forgets a Face' (New York Times, 13 July 2011), <https://www.nytimes.com/2011/07/14/world/asia/14identity.html>, accessed 10 April 2024.
[18] Mary Ellen O'Connell, 'Data Privacy Rights: The Same in War and Peace' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (NATO CCDCOE Publications 2022), 12-29, 13-14.
[19] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion of the ICJ) [2004] ICJ Rep 136, para 106.
[20] *Legality of the Use or Threat of Nuclear Weapons* (Advisory Opinion of the ICJ) [1996] ICJ Rep 226, para 24.
[21] *Hassan v. United Kingdom* (2014) ECHR 29750/09, (2014) 38 BHRC 358, [2014] ECHR 993, paras 101-106.
[22] See Andrew Clapham, 'Human Rights in Armed Conflict: Metaphors, Maxims, and the Move to Interoperability' (2018), 12 Journal of Human Rights and International Legal Discourse, 9-22.
[23] 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 (2022), 463-492, 464.

adequately protect these rights in the context of modern warfare.[24] The lack of detailed guidelines on data protection in conflict zones has resulted in extensive surveillance, and data collection that is justified without proper safeguards.[25] It also provides a degree of abuse in justifying extensive surveillance and data collection in conflict-affected zones.[26] For example, a recent study by Human Rights Watch on the violation of human rights by Israeli forces has stated that Israel has been using facial recognition in an attempt to monitor Palestinians in the territories of the West Bank without adequate supervision, leading to extensive surveillance and unauthorized use of personal information.[27] Therefore, the concern is not only the gaps in IHL and IHRL but also in the implementation of current regulations governing armed conflicts and technological advancements to protect the data and privacy of civilians affected by modern military technologies.

Whereas the use of surveillance technologies in modern IACs and occupied territories has increased significantly and represents a potential threat to civilians' data and their right to privacy, this thesis aims to address this *general question*: To what extent should existing IHL and IHRL frameworks be reformed to effectively safeguard civilians' data and privacy rights against the challenges posed by surveillance technologies, specifically surveillance drones and biometric data collection, in conflict zones and occupied territories?

For this purpose, I proposed to address four sub-questions. The *first sub-question* is: What are data, the right to privacy, data protection, surveillance drones, and biometric collection technologies? The *second sub-question* considers: What specific provisions under IHL and IHRL are designed to protect the right to privacy and data protection in conflicts and occupied zones, and where do these measures fall short and create gaps in securing civilians' privacy? To answer this question, I will examine key regulations, conventions, and treaties to clarify the position of these legal frameworks and the states' obligations to protect civilians' privacy rights. The *third sub-question* consists of: How do surveillance drones and biometric data collection technologies in the Russia-Ukraine conflict and the occupied territories of Palestine, respectively, challenge existing IHL and IHRL frameworks for privacy and data protection? This chapter aims to analyse the use of surveillance technologies in Ukraine and data collection technologies in Palestine to examine how they challenge existing protections for privacy and data. As the *fourth sub-question*, I will ask what legal adaptations are necessary to address the gaps that will be analysed in the second sub-question concerning the mentioned technologies in conflict-affected zones? This sub-question investigates the legislative modifications that are required to improve privacy safeguards in conflict-affected areas.

1.1 Scope

This thesis will focus on certain key elements, eliminating others to ensure the depth and feasibility of the study.

I mainly focus on legal gaps and state obligations. It is important because in modern IACs and occupied territories, technological advancements, especially in data surveillance, raise

[24] Watt (n 12), 159-160.
[25] *Ibid*, 160.
[26] *Ibid.*
[27] Human Rights Watch, 'A Threshold Crossed: Israeli Authorities and the Crimes of Apartheid and Persecution' (2021), 76 <https://www.hrw.org/report/2021/04/27/threshold-crossed/israeli-authorities-and-crimes-apartheid-and-persecution>, accessed 17 April 2024.

questions about the importance of the right to privacy during armed conflicts.[28] While the influence of non-state actors such as armed groups and corporations is growing in conflict zones, this thesis will only focus on states as high contracting parties to the GC I-IV and human rights conventions such as ICCPR.

Here, I intend to focus on the rights to data protection and privacy. Thus, further risks, such as cybercrime and espionage, are beyond the scope of this study. In this research, I will focus on IACs and occupations because the main focus of the research will be on states' obligations, and due to the use of new technologies in recent cases, the possibility of violating individuals' digital privacy rights has increased.

To clarify the word 'new technologies', in this thesis I will examine the impact of two kinds of technologies on civilians' privacy. The first category is surveillance drones, which are a kind of unmanned aerial vehicles (UAVs) equipped with cameras and sensors to monitor and gather data over specific areas, for military or intelligence purposes.[29] These are important in the context of this thesis because their widespread use in modern IACs has created a system of intense surveillance over the daily activities of civilians, exposing them to constant monitoring.[30] The second category is biometric data collection technology, which uses methods such as fingerprinting, facial recognition, and iris scanning to gather and store unique physical characteristics of individuals for identity verification and security purposes.[31] Although this category is relatively older, new updates and their broad function, especially in occupied territories, could be a tool to monitor a wide range of information, even more than civilians' fingerprints and faces.[32]

Moreover, this thesis will specifically analyse two case studies in the context of protecting the right to privacy. The primary case study centres around the Russia-Ukraine conflict, highlighting the prominent role of surveillance drones in military operations during this particular conflict.[33] The second case study is Palestine's situation, which is crucial to this study because there is a wide range of evidence of using data collection technologies in the occupied territories of Palestine, which threatens the civilians' privacy rights.[34]

As discussed earlier, this thesis aims to examine the civilians' right to privacy and data protection because during conflicts and occupations, little attention is paid to these civilians' rights, and the existing gaps in regulations and states' implementations could become a bias for violations of these rights and even the misuse of personal data for military purposes, which will be discussed in detail in the next chapters.

---

[28] Robin Geiss and Henning Lahmann, 'Protection of Data in Armed Conflict' (2021), 97 International Law Studies 556-572, 559.
[29] Watt (n 12), 16-162.
[30] *Ibid*.
[31] Arun Ross and Anil K. Jain, 'Biometric Recognition: Security and Privacy Concerns' (2003) 1(2) IEEE Security & Privacy 33-42, 34.
[32] See e.g. Rina Chandran, 'Afghans Scramble to Delete Digital History, Evade Biometrics' (Reuters, 17 August 2021),<https://www.reuters.com/article/afghanistan-tech-conflict/afghans-scramble-to-delete-digitalhistory-evade-biometrics-idUSL8N2PO1FH >, accessed 15 April 2024.
[33] Matt Burgess, 'Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory' (Wired, 27 February 2022, <https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/> ,accessed 12 April 2024.
[34] Lubin (n 23), 465.

1.2 Methodology

From a methodological point of view, I will use multiple methods to find the answer to the research question. First, I will apply a descriptive methodology to define the key concepts in this thesis. This approach is valuable in providing an extensive foundation for the research.

Second, an evaluative method will be applied to clarify the international regulations regarding digital rights, their adaptability to technological challenges, and the practical implementation of states' obligations. This approach is essential to recognize the shortcomings of existing legal frameworks and their difficulties in practice. It can also set the stage for the application of the normative approach. Furthermore, evaluating the two case studies will provide a clearer understanding of the existing gaps.

Third, I intend to compare IHRL with the European General Data Protection Regulation (GDPR), only in the context of states' obligations to protect the right to privacy in times of conflict. This could be useful to identify ways to fill the existing legal gaps, which is the main goal of this thesis.

Finally, to provide recommendations for reforming regulations regarding the existing gaps in protecting data and the right to privacy, the application of a normative approach is necessary. This method is based on an analysis of IHL and IHRL norms alongside the existing literature. This approach aims to propose enhancements to the existing regulations to ensure maximum protection of privacy rights. In this regard, the normative approach in this thesis will be based on the IHRL principle of human dignity, which recognizes the inherent worth of individuals and mandates protecting their intrinsic value.[35] Another basis is the IHL principle of constant care,[36] and the customary principle of precautions in attack, which require parties to a conflict to continuously ensure the protection of civilians and civilian objects by taking all feasible steps to avoid or minimize harm to them in military operations.[37] This thesis also mentions limited ethical considerations to strike a balance between states' security concerns and the right to privacy.

To answer the research question, this thesis proceeds as follows: Firstly, I will use the descriptive methodology to define the key concepts and clarify the relationship between the right to privacy and data protection. Secondly, I will examine the existing regulations under IHL to analyse its rules for privacy in conflict zones. Thirdly, I will focus on a more practical analysis of the challenges of the specified technologies in the case studies. Consequently, based on the challenges identified, filling the gaps in legal frameworks will be analysed. Finally, I will summarize the thesis findings in the conclusion.

---

[35] See Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/810 at 71 (1948), art 1; Geneva Convention (III) relative to the Treatment of Prisoners of War, 75 UNTS 135 (entered into force 21 October 1950), art 3.

[36] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1125 UNTS 3 (entered into force 7 December 1978), art 57(1).

[37] International Committee of the Red Cross, 'Rule 15: Precautions in Attack', Customary International Humanitarian Law Database (ICRC 2005),< https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15 >, accessed 15 April 2024.

2 Exploring Foundations: Privacy, Data Protection and Surveillance Technologies

In this chapter, I apply a descriptive methodology to examine three interlinked concepts that are the basis for understanding the existing legal deficiencies under IHL and IHRL to protect privacy rights: the right to privacy, data protection, and specified surveillance technologies. I initiate my analysis with the definition of the right to privacy and its scope in conflict zones. Then, I examine the definition of data and data protection and their link with the right to privacy. Finally, I will describe surveillance drones, biometric collection technologies, and their primary impacts on privacy. This chapter aims to provide an overview of the key terms through descriptive analysis, laying the foundation for further in-depth analysis of the legal concepts.

2.1 Definition and Interconnection

2.1.1 The Right To Privacy

The right to privacy is universally accepted as a fundamental human right to protect human dignity, which implies that individuals should be treated with respect and consideration.[38] This fundamental right is enshrined in several international frameworks. Mainly, Article 12 of the Universal Declaration of Human Rights (UDHR) states that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."[39] Additionally, Article 17 of the ICCPR uses the same words to clarify the definition of the right to privacy.[40] Moreover, this right has been emphasized in other regional and domestic legal documents. For example, Article 8 of the European Convention on Human Rights (ECHR), emphasizes that "everyone has the right to respect for his private and family life, his home, and his correspondence."[41]

The Human Rights Committee of the ICCPR, in its general comment No. 16, clarifies the scope of this right. The committee mentioned that protection of this right is crucial but could be relative; thus, interference could be possible if authorized clearly under valid regulations and if necessary according to the public interest.[42] As a result, the right to privacy is not an absolute right and could be restricted. Moreover, according to Article 4(1) of the ICCPR, states might be allowed to derogate from their obligations under human rights in cases of "public emergency."[43] One of these cases could be in the times of IACs and occupations. However, the committee declared that "not every single armed conflict, *ipso facto*, provides such conditions for derogation."[44] Hence, derogations should be limited and proportionate based on the case

[38]Human Rights Careers, 'Definitions: What is Human Dignity?' (Human Rights Careers) <https://www.humanrightscareers.com/issues/definitions-what-is-human-dignity/>, accessed 19 April 2024.
[39] United Nations General Assembly, Universal Declaration of Human Rights (UDHR) (10 December 1948), UN Doc A/RES/3/217 A, art 12.
[40] United Nations General Assembly, International Covenant on Civil and Political Rights (ICCPR) (16 December 1966), 999 UNTS 171, art 17.
[41] European Convention on Human Rights (ECHR) (opened for signature 4 November 1950, entered into force 3 September 1953), ETS No 5, art 8.
[42] Human Rights Committee, 'General Comment No 16: Article 17 (The Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation' (8 April 1988), UN Doc CCPR/C/GC/16, para 7.
[43] ICCPR (n 40), art 4(1).
[44] Human Rights Committee, 'General Comment No 29: Article 4 (Derogations during a State of Emergency)' (31 August 2001), UN Doc CCPR/C/21/Rev.1/Add.11, para 3.

conditions.[45] Therefore, the obligations to protect the right to privacy remain in place during the IACs, occupations and surveillance operations unless the circumstances require otherwise.

To support this, the judgment of the case of *Klass and Others v. Germany* recognized that while surveillance operations are necessary for security purposes, they must be balanced with robust protections to prevent misuse, affirming that any interference must be in accordance with the law.[46] Moreover, in the case of *Weber and Saravia v. Germany*, it has been emphasized that any surveillance must be legally prescribed, necessary, and proportionate to legitimate aims.[47]It stressed effective protection against possible abuses and highlighted the essential protections for privacy rights, even in national security situations.[48]

To comply with the ICCPR, there are several elements to ensure that the right to privacy is respected. In this regard, the committee stressed that:

> "[...]Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic, and other forms of communication, wire-tapping and recording of conversations should be prohibited. Searches of a person's home should be restricted to a search for necessary evidence and should not be allowed to amount to harassment. Effective measures should ensure that body searches are carried out in a manner consistent with the dignity of the person who is being searched."[49]

Furthermore, the right to privacy is considered a part of customary international law.[50] Although it is not easy to note with certainty how wide the boundaries of this customary right are, on a minimum basis, even the non-member states of the IHRL treaties cannot simply refuse their obligations to protect privacy, even in special circumstances such as armed conflicts.[51]

Privacy is a complicated concept with different dimensions. The right to privacy is also recognized in cyberspace and "is enforceable under international agreements."[52] Regarding the rapid advancements in technology, the meaning of the right to privacy has become broader. Therefore, there is a need for developed jurisprudence to reflect this evolving meaning. Such evolutions have created a related and closely associated right to privacy, which is data protection.[53] This concept will be studied in the next section.

2.1.2 Data and Data Protection

First, it is crucial to provide a general definition of data to understand the link between privacy and data protection. According to Article 4 of the GDPR, 'data' primarily refers to information including text documents, audio files, images or videos, software, etc.[54] Such information that is transferable is processed by computers and does not lose its quality or degrade with time.[55]

---

[45] *Ibid*, para 4.
[46] *Klass and Others v. Germany* (App no 5029/71) (1978) 2 EHRR 214, paras 49-50.
[47] *Weber and Saravia v. Germany* (App no 54934/00) (2006) ECtHR, 46 EHRR SE5, para 95.
[48] *Ibid*, para 95.
[49] General Comment No.16 (n 42), para 8.
[50] Alexandra Rengel, Privacy in the 21st Century (BRILL, Boston 2013), chapter 4, 108.
[51] *Ibid*, 107-108.
[52] Kriangsak Kittichaisaree, Public International Law of Cyberspace (1st ed, Springer International Publishing 2017), chapter 3, 57.
[53] *Ibid*, 55-57.
[54] General Data Protection Regulation (GDPR), 2016/679 of 27 April 2016, OJ L 119/1, art 4.
[55] Brian Pickle, 'Data Definition' (13 December 2022),< https://techterms.com/definition/data#google_vignette>, accessed 1 May 2024.

Furthermore, based on the definition provided by the OECD, "data is the physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means."[56]

The data can be categorized in various ways, such as nominal data, factual data, commercial data, AI-generated data, etc.[57] In this research, the main focus is on the right to privacy of civilians, with a specific emphasis on 'personal data'. Personal data encompasses personal information such as letters, diaries, names, biometric data, locations, network information, etc.[58]

'Data protection' refers to legal measures implemented to protect personal information from unauthorized access, including misuse of military objectives and disclosure even in occupied territories and during IACs.[59] There is a debate on whether the right to protection has been recognized universally; however, some scholars believe that this right might be a derivative of the right to privacy.[60] They refer to general comment No. 16 to support their argument, which states that "the gathering and holding of personal information on computers, data banks, and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."[61]Moreover, several cases support this argument. For example, in the case of *Z v. Finland*, the ECtHR stated that it is important to protect personal data as a part of the right to privacy.[62] Therefore, the right to data protection, at least according to the existing IHRL framework, is not separate.

However, at the international level, several examples implicitly recognize this right separately. For instance, states that have approved the UN Conference on Trade and Development (UNCTAD) have obligations to make laws for data protection.[63] In addition, the UN General Assembly (UNGA) requires the states to consider its guidelines to provide a comprehensive legal system for data protection.[64]

Furthermore, the right to data protection has been recognized separately in some regional legislation. For example, states parties to the Council of Europe Convention for Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) agreed to legislate to protect personal data.[65] The Charter of Fundamental Rights of the European Union also recognized this standalone right for the first time.[66]

---

[56] UNECE, Conference of European Statisticians Statistical Standards and Studies – No. 53, 'Terminology on Statistical Metadata' (Geneva, 2000), 42 < https://unece.org/DAM/stats/publications/53metadaterminology.pdf > , accessed 1 May 2024.
[57] *Ibid*, 42-43.
[58] GDPR (n 54), art 4.
[59] Kittichaisaree (n 52), 58.
[60] Lubin (n 23), 474.
[61] General Comment No.16 (n 26), para 10.
[62] *Z v. Finland* App no 22009/93 (ECHR, 25 February 1997), para 95.
[63] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide (2020), < https://unctad.org/page/data-protection-and-privacy-legislation-worldwide >, accessed 1 May 2024.
[64] UNGA, 'Guidelines for the Regulation of Computerized Personnel Data Files' Res 45/95 (14 December 1990), UN Doc A/RES/45/95, 45th sess, 1990-1991, para 4.
[65] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, 1981), art 4.
[66] Charter of Fundamental Rights of the European Union (2000/C 364/01), art 8.

Furthermore, the most important source concerning this area is the GDPR, which has been in force since 2018.[67] The GDPR serves substantial worth in the sense that it lays first protection rights for data, as laws in the Member States of the EU need to adhere to it.[68] It controls the processing with some principles, such as transparency and accountability in data control.[69] Also, the GDPR makes sure that the regulation is properly enforced to be implemented strictly as well.[70] For example, Google was fined €50 million in France due to non-compliance with the GDPR.[71] Hence, some scholars have argued that GDPR is important in incorporating international data protection standards, especially because of its extra-territorial nature and impact on non-European countries.[72]

According to such regulations, the right to privacy and data protection are two separate rights. Although these two are related and sometimes overlap, they cannot be used interchangeably. The right to data protection is about the processing of an individual's data, but the right to privacy, as stated in Article 17 of the ICCPR, is based on protecting people from interference in their private lives.[73] Subsequently, there is a nuanced distinction between these two fundamental rights, which should be considered when examining the application of these rights under IHL in conflict zones and occupied territories.

Comparatively, the right to data protection could also be restricted, which might be justified by referring, for example, to public interest and security issues such as conflicts. However, likewise, the right to privacy, restriction, and derogation of this right should be necessary, proportionate, and well justified under clear domestic rules.[74]

2.2 Surveillance Technology

2.2.1 Surveillance Drones

Before exploring drones, it could be useful to define surveillance. Based on existing literature, surveillance can be generally understood as an activity that consists of watching over a target for a constant period, where the target might be a human.[75]

Surveillance drones are known as a kind of UAVs, which are aircraft without onboard operators.[76] Such drones can be controlled remotely or operated based on automatic computer programs, and according to the recent production of advanced versions of these drones, they can carry different equipment, such as cameras and communication tools.[77] The use of these drones has increased in recent decades. For instance, until 2014, around 50 countries confirmed

[67] GDPR (n 54), art 1.
[68] Christopher Kuner, 'The GDPR: Implementation and International Implications' (2019) 25 International Data Privacy Law 7, 8.
[69] *Ibid*, 8.
[70] *Ibid*, 9.
[71] Elisa Bertino and Lorenzo Martino, 'Privacy and Security in the European Union: User Rights and Enforcement' (2019) 15 Journal of Cybersecurity 145, 150.
[72] *Ibid*.
[73] Kittichaisaree (n 52), 59.
[74] *Ibid*, 60-62.
[75] Roger Clarke, 'What Drones Inherit from Their Ancestors' (2014) 30 Computer Law and Security Review 247, 258.
[76] Markus Wagner, 'Unmanned Aerial Vehicles' in Anne Peters and Rüdiger Wolfrum (eds), Max Planck Encyclopedia of Public International Law (Oxford University Press, updated September 2014), 2-3.
[77] *Ibid*, 2-3.

the existence of this type of drone among their equipment.[78] These drones can be used for different purposes. In this thesis, the focus will be on their military use. Their military function is categorized into two different applications: 1) as a weapon for targeting objects, and 2) for surveillance and intelligence gathering purposes.[79] The challenges of the latter will be analysed in Chapter 4.

However, the use of such drones has its impacts on privacy issues. UAVs with sophisticated sensing and imaging capabilities can collect extensive personal data beyond what is allowed by IHRL regulations and without permission.[80] Due to the capabilities of this equipment to collect data, its deployment should specifically comply with the privacy regulations under ICCPR.[81] The privacy issues could become more significant in security contexts, especially in conflict zones or sensitive regions, because misuse of these drones for civilians' data in military operations and civilians' concerns about being under surveillance will increase.[82] For instance, in the recent conflict between Russia and Ukraine, Russian Orlan-10 drones were used to gather intelligence; however, they collected a wide range of civilians' data besides military data, which directly affected the privacy of local civilians in Ukraine.[83]

Although there are various regulations to protect civilians in conflict zones and occupied territories under IHL, civilians' privacy concerns are not addressed properly, and these regulations do not provide solutions to deal with the effects of these tools on privacy issues, mainly because they were adopted before these technological advancements.[84] Therefore, there is a need to analyse the IHL regulations to strike a balance between security concerns and civilian privacy issues.

2.2.2 Biometric Collection Technology

Biometric data encompasses various unique individual identifiers, such as fingerprints, DNA samples, voice recordings, and face images, which are collected by both government and private entities using diverse methods.[85] There is no question that the collection of such data is an essential requirement for states' security and is justified by acceptable legal reasons; however, the protection of such data is also required by human rights.[86] Therefore, state agencies should ensure that the privacy of biometric data is protected and that they do not provide access to other states, military groups, or companies for military purposes.[87]

The importance of biometric privacy increases when a security issue arises because biometrics fall under the category of sensitive data.[88] In this thesis, the issue of protecting biometric data will be analysed in a limited way, specifically in the occupied territories of Palestine. This is

[78] *Ibid*, 2.
[79] *Ibid*, 4.
[80] *Ibid, 5.*
[81] *Ibid*, 5-6.
[82] Watt (n 12), 158.
[83] Ulrike Franke, 'Drones in Ukraine and Beyond: Everything You Need to Know' (European Council on Foreign Relations, 11 August 2023), <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>, accessed 30 April 2024.
[84] Watt (n 12), 159-160.
[85] Pope, Carra, 'Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data' (2018), 26 Journal of Law and Policy 769-204, 772.
[86] *Ibid*, 775.
[87] *Ibid*, 771-773.
[88] *Ibid*.

mainly because there are a large number of biometric checkpoints where Palestinians must undergo fingerprint and facial recognition checks.[89] Although some of these measures are justified based on security grounds, there are still significant privacy concerns about freedom of movement and potential discrimination.[90] Moreover, there is a relationship between collecting biometric data and surveillance drones, where the drones can use biometric data to monitor civilian objects.[91]

Thus, there is a need to balance security concerns with privacy concerns, especially in occupied territories where, under the Hague Convention, the occupier state has to ensure public safety[92] while also being required to respect honour and family rights under IHL.[93] In the next chapter, the application of the right to privacy and data protection will be examined under the IHL framework to recognize if there is any gap in protecting these rights.

3 Application of Privacy Rights in Conflict-Affected Areas: An Analysis of IHL and IHRL

In the context of armed conflicts, the value of privacy rights is usually overshadowed by more immediate concerns, such as civilians' physical safety and territorial sovereignty.[94] However, even in times of conflict or occupation, these factors are crucial to maintaining individuals' autonomy and sense of dignity. Although IHRL provides a framework for protecting privacy rights, there are still shortcomings, specifically regarding data protection.[95] Similarly, IHL lacks explicit provisions to protect privacy rights, which complicates its application with new technologies, especially surveillance drones.[96] In this chapter, I aim to investigate the regulations under IHL for civilians' privacy in conflict-affected areas to determine to what extent IHL is primarily concerned about the privacy rights of civilians and what are the shortcomings under IHL and IHRL, especially regarding the recent use of military technologies such as surveillance drones. Therefore, first I will analyse the intersection of IHL and IHRL in conflict-affected areas. Then, I will analyse the IHL provisions on privacy rights and their shortcomings. Consequently, I will identify states' obligations and limitations under the IHRL framework. I will compare states' privacy rights obligations in IHRL with GDPR, which several scholars believe is a successful system because it consists of clear regulations and a suitable enforcement and implementation system.[97]

3.1 The Intersection of IHL and IHRL in Protecting Human Rights

First, it is crucial to clarify what legal frameworks are applicable to protect human rights in times of IACs and occupation.

---

[89] Lubin (n 23), 484.
[90] *Ibid.*
[91] Watt (n 12), 160.
[92] Hague Convention No. IV Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910), 36 Stat 2227 TS No 539, art 43.
[93] Geneva Convention IV Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287 (GCIV), art 27.
[94] Lubin (n 23), 464-465.
[95] Watt (n 12), 158-160.
[96] *Ibid*, 167.
[97] Bertino and Martino (n 71), 150-151.

IHL mainly aims to control the effects of armed conflicts by restricting warfare means and methods and protecting civilians and individuals who do not participate in hostilities.[98] In contrast, IHRL is the body of international law establishing states' obligations to respect, protect, and fulfill human rights.[99] Hence, IHL and IHRL are separate bodies of international law and differ in application. IHRL is applicable in peacetime, while IHL is designed to operate during armed conflicts and occupations. However, it has been recognized that these bodies of international law have a 'complementary nexus' in situations of conflict and occupation.

In this regard, the ICJ in the *Nuclear Weapons Advisory Opinion*[100] and the *Wall Advisory Opinion*[101] stressed that during armed conflicts, the protection of human rights continues. Moreover, the human rights committee in general comment No. 31 elaborated that "the ICCPR applies also in situations of armed conflict to which the rules of international humanitarian law are applicable."[102] It also mentioned that IHL and IHRL have a 'complementary relationship'.[103] The *Wall Advisory Opinion* focused on the situation of occupation and emphasized that due to the effective control of the occupying state, the majority of human rights, including privacy rights stated in the ICCPR, must be applied.[104] The ECtHR, in the case of *Al-Skeini v. United Kingdom*, issued a similar decision in its judgment on the occupied zones in Iraq.[105] Although the application of human rights is more complicated under active IACs, the result of the application of rights such as privacy rights is the same in IACs and occupied zones.[106]

Moreover, concerning the complementary application of IHL and IHRL in conflict-affected areas, the International Committee of the Red Cross (ICRC) has stated:

"[I]t is generally agreed that IHL and human rights law are complementary legal frameworks, albeit with different scopes of application. While most rules of the IHL apply only during armed conflicts, human rights law applies at all times. Therefore, in times of armed conflict, certain norms of the two regimes overlap, sometimes revealing a gap in humanitarian law."[107]

However, there are still certain debates on the application of these frameworks and solutions for the possible normative conflicts between these rules. Some scholars state that in armed conflicts and occupations, IHL acts as a *lex specialis* and has priority in application over the

[98] Geneva Convention I-IV (1949), common art 2.
[99] See for example, ICCPR (n 40), art 2(3); UDHR (n 39), art 1.
[100] *Legality of the Use or Threat of Nuclear Weapons* (n 20), para 24.
[101] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (n 19), para 106.
[102] U.N. Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13, para 11.
[103] *Ibid.*
[104] Ellen O'Connell (n 18), 23.
[105] *Al-Skeini v. United Kingdom* (2011) 53 EHRR 589 (ECtHR), para 137.
[106] Ellen O'Connell (n 18), 23-24.
[107] International Committee of the Red Cross, 'Strengthening Legal Protection for Persons Deprived of their Liberty in Relation to Non-International Armed Conflict: Regional Consultations 2012–13' (2013), 5 <https://www.icrc.org/en/doc/assets/files/2013/strengthening-legal-protection-detention-consultations-2012-2013-icrc.pdf >, accessed 4 May 2024.

use of IHRL.[108] In contrast, some other scholars state that IHRL is an interpretive and complementary tool for filling gaps in IHL.[109]

Nonetheless, even the complementary nexus between these bodies of international law is usually considered in certain rights, such as the right to life and the prohibition of arbitrary detention.[110] However, the context of data protection and privacy rights in IACs and occupations is complicated, mainly because IHL applies as the main legal framework in such situations. Still, under IHL, the problem of protecting civilians' data is not addressed explicitly and directly, and as noted before, IHRL also does not impose specific regulations, specifically on data protection.[111] In addition, IHRL rules on the right to privacy, due to the development of new surveillance technologies, have not changed significantly to regulate them, which will be analysed in the next section.

3.2 Analysis IHL Provisions for the Protection of Privacy and Personal Data

IHL is mainly articulated through the GCs and their Additional Protocols (AP I and II). These documents regulate the obligations of occupying forces and combatants to ensure the protection of civilians and those hors de combat.[112] These regulations also govern the conduct of IACs and NIACs in addition to occupation.[113] In this section, the focus is on the extent of primary protection of civilian privacy rights in IACs and occupied territories under IHL. Thus, the Fourth GC (GC IV)—relative to the protection of civilian persons in times of war—and the AP I—relating to the protection of victims of IACs—will be examined. GC IV and AP I mention no explicit rules to protect privacy because the last codifications in the IHL refer to the 1970s.[114] However, it cannot be denied that the IHL provisions are deeply rooted in the principle of human dignity, from which the right to privacy is also derived. In this regard, some scholars refer to the principle of distinction and the prohibition on causing unnecessary suffering under IHL, which impose obligations not to target civilians and civilian objectives and prohibit causing more suffering than is required for achieving a military objective, respectively.[115]

Under IHL, a few provisions implicitly refer to privacy and data protection. Article 27 of the GC IV generally sets the basis for the treatment of protected individuals, including civilians, which is potentially related to the right to privacy.[116] Article 27 basically ensures respect for individuals' honour and family rights, which is similar to Article 46 of the Hague regulations, which have protections against "arbitrary interference in the home and marriage

[108] William Schabas, 'Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum' (2007) 40(2) L Rev, 592, 592-593.
[109] See for example, Oona A Hathaway et al, 'Which Law Governs During Armed Conflict—The Relationship Between International Humanitarian Law and Human Rights Law' (2012) 96(6) Minn L Rev 1883.
[110] Watt (n 12), 167.
[111] *Ibid*.
[112] Crawford and Pert, (n 10), 33.
[113] *Ibid*, 35.
[114] Lubin (n 23), 464.
[115] See for example, Eyal Benvenisti, 'Human Dignity in Combat: The Duty to Spare Enemy Civilians' (2006) 39:2 Israel Law Review 81, 85-90; Ibid, 470-472.
[116] GC IV (n 93), art 27: "Protected persons are entitled, in all circumstances, to respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. They shall at all times be humanely treated, and shall be protected especially against all acts of violence or threats thereof and against insults and public curiosity."

ties."[117]Additionally, Article 27 mandates "human treatment" for protected individuals in occupied territories.[118] Besides, Article 53 of GC IV prohibits unnecessary and unlawful destruction of private properties by occupying power.[119] Moreover, Article 31 of GC IV prohibits the occupier from using "physical or moral coercion to collect data from protected individuals."[120] However, these regulations are not completely clear regarding the protection of civilians' privacy. Indeed, these provisions are limited to certain boundaries, such as the protection of home privacy, and it is hard to interpret them in various aspects, such as personal data.

Concerning personal data, different articles in GC IV stress the protection of various aspects of medical services, including hospitals and medical staff.[121] Several scholars argue that it is possible to extend this protection to personal medical data.[122] Based on this argument, these scholars admit that it is also possible to extend this protection for personal medical data to all personal data. They provide support for this argument emphasizing that the importance of human dignity in both medical and non-medical data is equal.[123] In contrast, other scholars argue that other kinds of personal data are excluded from protection because GC IV mentioned medical data as a specific category, and other categories are excluded.[124] Thus, according to this view, it is hard to extend the protection of medical services under IHL to all personal data.

Furthermore, Article 52 of AP I aims to generally protect civilian objectives from targeting. In this regard, it was emphasized that "civilian objects shall not be the object of attack or reprisals; civilian objects are all objects that are not military objectives."[125] However, there is a certain debate about whether personal data is also considered a civilian objective. Most scholars argued that data could not be an object under IHL because it has no physical dimension.[126] They support their argumentation by referring to the treaty interpretation rules under Articles 31-33 of the Vienna Convention on the Law of Treaties and believe that since data is intangible, it does not fit the meaning of 'object' offered in the ICRC commentary.[127] Additionally, according to state practice, an object under IHL is a physical thing.[128] Thus, protecting civilian objectives under IHL, does not apply to personal data. Therefore, IHL provides basic guidelines for protecting human dignity, but it needs to go further in protecting privacy, especially in the context of personal data in the digital age.

---

[117] Omar Yousef Shehabi, 'Digital Privacy and Data Protection in Military Occupation' in R Buchan and A Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022) 87-112, 96; Hague Convention (n 92), art 46.
[118] *Ibid*, 98-99; GC IV (n 93), art 27.
[119] GC IV (n 93), art 53: "The Occupying Power may not compel protected persons to serve in its armed or auxiliary forces. No pressure or propaganda which aims at securing voluntary enlistment is permitted."
[120] *Ibid*, art 31.
[121] See for example, GC IV (n 93), arts 18-22.
[122] Geiss and Lahmann (n 28), 565.
[123] *Ibid*.
[124] *Ibid*, 25.
[125] AP I (n 36), art 52.
[126] Ori Pomson, ''Objects'? The Legal Status of Computer Data under International Humanitarian Law' (2023) 28(2) Journal of Conflict and Security Law 349-387, 350.
[127] *Ibid*; See also Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Martinus Nijhoff 1987) 166.
[128] Pomson (n 126), 386-387.

3.3 Comparative Analysis of States' human rights Obligations for Privacy and Data Protection under IHRL and GDPR

3.3.1 IHRL

As discussed in previous sections, IHL provides limited regulations for protecting privacy and data, and even these few provisions are not explicit. Therefore, there is a debate on the applicability of IHL provisions to the right to privacy, making it less comprehensive for states to protect them or provide compensation in cases of violations during AICs and occupations.[129] For instance, Article 91 of AP I states that "a party to the conflict that violates the provisions of the Conventions or of this Protocol shall if the case demands, be liable to pay compensation."[130] Nevertheless, as privacy is not explicitly discussed under IHL, it becomes limited to providing remedies for violating privacy and data protection as human rights.

According to the dual application of IHL and IHRL in times of IACs and occupation, for understanding states' obligations, IHRL regulations should be examined as a complementary tool. IHRL has a significant role in protecting civilians during armed conflict by offering positive legal responsibilities for the states, such as preventing violations, investigating alleged breaches, and providing redress for victims.[131]

Generally speaking, under IHRL, states primarily must provide people on their territory with human rights commitments.[132] However, in the context of IACs and occupations, it is under question whether human rights obligations are applicable beyond the territories of states. Generally, when a state has effective control over a foreign territory or people who live in that territory, their human rights obligations spread beyond its boundaries into the area under its effective control.[133] Therefore, the state that has effective control must provide legislation to protect human rights and suitable remedies for violations. For example, in the case of *Al-Skeini v. United Kingdom*, the ECtHR decided that the UK's human rights obligations extended to individuals detained by British forces in Iraq, as the UK had effective control over the area.[134]

However, under IHRL, states might derogate their obligations under certain circumstances or apply limitations on relative rights justified by rules. As stated in Chapter 2, the right to privacy under Article 17 of the ICCPR is not absolute.[135] Thus, states in certain situations can derogate from their obligations to protect this right based on Article 4 of the ICCPR.[136]

However, to justify derogations, two conditions must be met. First, derogation is only possible in "public emergencies that threaten the life of the nation."[137] IACs could be considered an emergency, but they must threaten the nation. Second, these derogations must be officially declared by the state and be temporary.[138] Moreover, this state should inform the UN secretary general of this decision to allow the human rights committee and other states to monitor the

[129] Watt (n 12), 169-170.
[130] AP I (n 36), art 91.
[131] Clapham (n 22), 12.
[132] Watt (n 12), 170.
[133] See *Wall Advisory Opinion* (n 19), para 107-113; General Comment No. 31 (n 102), para 10.
[134] *Al-Skeini v. United Kingdom* [2011] (n 105), para 138.
[135] ICCPR (n 40), art 17.
[136] ICCPR (n 40), art 4.
[137] *Ibid*, art 4(1).
[138] *Ibid*.

compliance with the ICCPR.[139] Currently, no state has derogated from Article 17 due to engagement in an armed conflict.[140]

In addition to derogations, states might use 'permissible limitations' in their human rights obligations, which must be justified for important purposes, such as national security and public safety.[141] However, these limitations also must be specified under domestic law and be reasonable and proportionate.[142] States often prefer to use these limitations because they justify that they have easier conditions and do not need to declare officially or meet the conditions of Article 4 of the ICCPR.[143] Furthermore, IHRL requests states to ensure providing remedies for those individuals whose rights have been violated.[144]

The applicability of derogations and limitations in IACs and occupations must be scrutinized to ensure they do not disproportionately affect the rights of civilians. For example, in the case of *Hassan v. United Kingdom*, the ECtHR recognized the need to address how human rights protection should be applied regarding the nature of conflicts, emphasizing that the ECHR is applicable in an extraterritorial mode when a state has effective control.[145] This case highlights that while IHRL allows for certain derogations and limitations, these cannot easily be applied and must be necessary, proportionate, and respect the essence of human rights.[146] However, almost all major of these cases support the right to life, non-arbitrary detention and freedom of movement, but privacy rights have not received much attention.

Although states have a challenging commitment to balance their human rights obligations and security concerns, especially in the context of armed conflicts and occupations, the permissible limitations grant them significant flexibility in deciding how to implement their human rights obligations.[147] Finally, as Watt affirms, states in armed conflicts and occupations often underestimate their obligations to protect privacy and personal data in current frameworks because their obligations under *jus in bello* are likely more urgent, and privacy obligations are not strong enough.[148] Therefore, the current protection of data and privacy under IHL and IHRL is inadequate because they do not sufficiently address the issues of the protection of these rights during conflicts and occupations.

3.3.2 GDPR

GDPR is a regional legislation in the EU that addresses the guidelines for safeguarding EU personal data subjects.[149] Furthermore, based on Article 3, the GDPR applies to non-EU entities that process data of EU citizens, as confirmed in the case of *Google LLC v. CNIL*.[150] This ensures robust data protection of high quality, regardless of where the data controller is located.

---

[139] *Ibid*, art 4(3).
[140] Watt (n 12), 171.
[141] See for example, ICCPR (n 40), arts 12(3), 18(3) and19(3).
[142] General Comment No.16 (n 42), para 3 ; Concluding Observations of the UN Human Rights Committee on Switzerland is: UN Human Rights Committee, Concluding Observations on the Fourth Periodic Report of Switzerland, issued on July 27, 2017, UN document number CCPR/C/CHE/CO/4, para 46.
[143] Watt (n 12), 173.
[144] ICCPR (n 40), art 2(3); UDHR (n 23), art 8.
[145] *Hassan v. United Kingdom* (n 21), paras 74-78.
[146] *Ibid*, paras 102-106.
[147] Watt (n 12), 173-174.
[148] *Ibid*, 174.
[149]Anel Roos, 'Data Protection Principles under the GDPR and the POPI Act: A Comparison' (2023) 86 Romeins-Hollandse Reg 1, 1-26 (Hein Online), 2.
[150] *Google LLC v. CNIL* (Case C-507/17), [2019] ECLI:EU:C:2019:772, paras 44-45.

The scope of GDPR in comparison to IHRL, is narrower because it mainly focuses on data protection rights; however, it provides valuable principles in the context of data protection that could be useful to clarify the normative gap under IHRL.

It should be noted that the GDPR is applicable even in emergencies such as conflicts; however, the GDPR recognizes exceptional circumstances for protecting personal data, such as public interests, but limits it based on proportionality and necessity.[151] Hence, the protection of data under the GDPR must not cease in times of conflict without proper justification, as required under Articles 6 and 9.[152] Furthermore, the obligations under GDPR apply to the private sector, i.e., business companies, and public authorities, known as 'data controllers'.[153]

GDPR introduces several principles for personal data protection, but what distinguishes GPDR is its consideration of a comprehensive system for the responsibility and accountability of data controllers. This can be understood from the four main principles of GDPR.

First is the principle of *lawfulness, fairness, and transparency*, which expresses that personal data must be processed and treated legally, fairly, and transparently concerning the data subject.[154] Data processing must be based on limited legal foundations and justified by the rule of law.[155] Hence, in collecting personal data, the controller must provide the data subject with contact information, its representative, and the data protection officer.[156] Moreover, the main goal and the legal foundation for this processing must also be disclosed to the data subject.[157] The controller shall also notify data subjects about the duration of data storage and the factors used to decide this timeframe.[158]

Second is the principle of *purpose and storage specification and limitation*, which stresses that personal data should only be used for specific and legitimate purposes indicated at the time of collection.[159] In this regard, the controller is responsible for providing a legitimate purpose for subsequent and further processing of personal data.[160] Moreover, personal data should be kept no longer than the logical timeframe that is required for the initial purpose of data collection and processing, and the controller is responsible for indicating this timeframe.[161]

Third is the principle of *integrity and confidentiality*, which states that personal data should be safeguarded with proper security measures to prevent unauthorized access, use, or destruction of data.[162] Moreover, the controller is required to conduct a risk assessment involved in processing data, such as unlawful destruction.[163] The controller is also responsible for mitigating such risks and shall employ a processor with enough guarantees to implement the necessary technical and organizational steps to fulfill regulatory requirements.[164] Furthermore,

[151] Lubin (n 12), 474-476.
[152] GDPR (n 54), arts 6, 9.
[153] *Ibid*, art 24, 25.
[154] Roos (n 149), 5-6.
[155] Lubin (n 23), 476.
[156] Roos (n 149), 7 ; GDPR (n 54), art 13(1).
[157] *Ibid*.
[158] *Ibid*, 7-8.
[159] *Ibid*, 15.
[160] *Ibid*.
[161] GDPR (n 54), art 5(1)(e).
[162] Roos (n 149), 16.
[163] *Ibid*, 16-17.
[164] *Ibid.*

the controller must notify the supervisory authority of any security breach involving personal data within a reasonable time frame.[165]

Fourth is the principle of *accountability*, which establishes that to guarantee compliance with data protection standards, data controllers and processors should be subject to due process, oversight, and possible legal sanctions, such as through a data protection authority.[166] The accountability concept includes legal remedies for data subjects whose rights have been violated and consequences for data controllers who do not comply with the regulations.[167] The GDPR guarantees the right to file a complaint with a supervisory authority, as well as the right to an appropriate legal remedy against a controller.[168] Moreover, a supervisory authority or a member state could impose administrative fines or penalties for violating requirements under GDPR.[169]

Although the GDPR process seems rather complicated, the proportionality and necessity principles allow for flexibility. Articles 6 and 9 permit the exceptions made for public interest or vital interest, which make the requirement of data protection both feasible and pragmatic in an emergency, such as a conflict.[170] Overall, the GDPR, in the narrow context of data protection, mandates a more comprehensive and enforceable system of obligations and responsibilities that could be inspired to fill the IHRL gaps to fulfill data protection rights and even provide an enhanced system of state obligations for protecting privacy and its limitations.

In the next chapter, I will examine two cases in IACs and occupied territories to show how the use of some new surveillance technologies poses challenges for the IHL and IHRL regulations in protecting civilians' data and privacy.

4 Navigating Surveillance: Drones and Biometrics in Conflict-Affected Areas Privacy Challenges in Ukraine and Palestine

In recent decades, one of the most significant impacts on the evolution of modern warfare has been the use of new technologies in the context of occupation and armed conflicts, especially the emergence of surveillance drones and the massive collection of civilian biometric data. The use of these technologies has posed new challenges that the current human rights regime struggles to deal with. Surveillance drones can provide a widely accessible intelligence gathering system, and new biometric collection technologies can extract personal data to be analysed.[171] Although such technologies might have security benefits for states, they entail different legal and ethical challenges, with a particular emphasis on the infringement of privacy rights.[172] Such concerns could pose more challenges because, as discussed in the previous chapter under IHL and IHRL, there are normative gaps in protecting personal data and privacy rights.

[165] GDPR (n 54), art 33.
[166] Roos (n 149), 21-22.
[167] Lubin (n 23), 478.
[168] GDPR (n 54) arts 77, 79.
[169] *Ibid*, art 84.
[170] *Ibid*, arts 6, 9.
[171] See generally Dominika Kunertova, 'Drones have boots: Learning from Russia's war in Ukraine' (2023) 44(4) Contemporary Security Policy 576-591.
[172] *Ibid*.

In this chapter I aim to analyse two case studies in the context of using new technologies in conflict-affected areas for more clarification of the need for evolved regulations to govern privacy rights. First, I will give a general overview of the increasing use of such technologies in conflict-affected zones. Second, I will critically examine the challenges of surveillance drones in the Russia-Ukraine conflict and biometric collection in occupied Palestine. Finally, I will conclude that these challenges justify the need for normative updates in IHL and IHRL.

4.1 Overview of the Use of Surveillance Technologies in Conflict-Affected Areas

Surveillance drones have a considerable impact on the nature of military operations by observing and neutralizing targets and objects of military importance, as well as strategic and operational reconnaissance, detection of enemy conduct, and identification of legitimate targets.[173] The legality of the surveillance drones' function for targeted killings is still controversial, especially under IHRL.[174] However, as discussed in Chapter 2, the legality of their function in intelligence gathering has not been widely considered under regulations and state practices. Nevertheless, these technologies are widely used for surveillance purposes. For example, according to reports, in addition to the United States, the United Kingdom, Israel, Russia, and France, twenty-nine other states are developing new generation armed drones for surveillance and distance targeting.[175] UAVs are equipped with high-tech tools such as face recognition software and GPS trackers. They can continuously monitor potential targets and gather data, which is then stored in military databases and shared with armed forces and intelligence agencies, which facilitate states' operations, especially during conflicts and occupations.[176] For instance, the United States, after the withdrawal of American troops from Afghanistan, emphasized its ongoing strategy of engaging in future conflicts more remotely, which had already been in use.[177]

Biometric data gathering tools provide minute details of individuals' data in conflict-affected areas. Such collected data is then employed for monitoring motions and confirming identities.[178] The use of this type of data is accepted for security purposes, such as verifying the identity of combatants; however, the excessive gathering of biometric data will result in privacy violations and potential information abuses.[179]

Additionally, the interaction between the biometric data collection and the constant monitoring function of the drones creates a multi-dimensional security grid that strengthens the precision of possible threat perception.[180] The use of collected biometric data, specifically in the context of occupied zones could raise ethical concerns regarding civilians' privacy. Using surveillance

---

[173] Peter Bergen et al, World of Drones, New America (30 July 2020) <https://www.newamerica.org/international-security/reports/world-drones/>, accessed 15 May 2024.
[174] Council of Europe, 'Drones and Targeted Killing: The Need to Uphold Human Rights and International Law' Doc No 13731 (2015), para 18.
[175] Bergen et al (n 173).
[176] Watt (n 12), 160.
[177] Remarks by President Biden on the End of the War in Afghanistan, The White House (31 August 2021) <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/>, accessed 15 May 2024.
[178] See generally Usama Halabi, 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel', in Surveillance and Control in Israel/Palestine: Population, Territory and Power, (Elia Zureik, David Lyon, and Yasmeen Abu-Laban eds, 2010), 210-211.
[179] *Ibid.*
[180] Yousef Shehabi (n 117), 95.

technologies such as facial recognition checkpoints could reinforce the occupier's powerful human and signal intelligence infrastructure, mainly analysing communications within the occupied region.[181] For example, in the occupied territories of Palestine, Israel is consolidating its control over the region by generating a data trail of movement across 'land cells' that are formed by checkpoints to inhibit movement entirely by 'exclusionary surveillance', as described by Ariel Handel.[182] Such surveillance technologies are considered an intrinsic feature of the "Israeli separation associated regime, which the ICJ stated gravely infringes on several Palestinian rights."[183] Furthermore, surveillance technology in occupied territories can create a divided society and put more mental strain on civilians.[184]

4.2 First Case: Surveillance Drones in the Russia-Ukraine Conflict

Russia launched a complete invasion of Ukraine in February 2022, constituting a highly consequential threat in Europe after the Cold War.[185] After years of tension between Russia and Ukraine since 2014, which was rooted in the annexation of Crimea, the conflict escalated through Russian military activities in eastern parts of Ukraine, specifically in Donetsk and Luhansk.[186] This conflict, which according to Common Article 2 of the GCs is an IAC,[187] soon became the focal point of tensions between Russia and Western states, especially the NATO members.[188] It has had significant implications for international security, as well as a severe humanitarian crisis, including thousands of fatalities and an escalation in the refugee crisis in Europe.[189] One of its important dimensions is the high rate of use of new military technologies during the armed conflict by both parties involved. Many warfare and security experts have affirmed that this conflict is a clear example of how modern technology has transformed conventional combat.[190] For instance, according to existing reports, the Ukrainian battlefield displays the most intense employment of different kinds of drones in military combat in history.[191]

Since the start of a new wave of the conflict in 2022, both involved states have used drones for intelligence gathering and targeting.[192] On the one hand, Ukraine uses cheap and small drones, particularly the First-Person View drones (FPV).[193] Such drones were initially designed for

[181] *Ibid*, 93-95.
[182] Ariel Handel, 'Exclusionary Surveillance and Spatial Uncertainty in the Occupied Palestinian Territories', in Elia Zureik, David Lyon, and Yasmeen Abu-Laban (eds), Surveillance and Control in Israel/Palestine: Population, Territory and Power (2010) 259, 270.
[183] *Wall Advisory Opinion* (n 19), para 193.
[184] Watt (n 12), 162-163.
[185] Mohamad Albakjaji and Reem Almarzoqi, 'The Impact of Digital Technology on International Relations: The Case of the War between Russia and Ukraine' (2023) 2 Access to Justice in Eastern Europe 8, (Hein Online), 8-24, 10.
[186] *Ibid*, 14-15.
[187] GC Common art 2, (n 98).
[188] W. Casey Biggerstaff, 'Can Aid or Assistance Be a Use of Force?: Expert Q&A from Stockton Centre's Russia-Ukraine Conference' (Just Security, 2 March 2023),<https://www.justsecurity.org/85336/can-aid-or-assistance-be-a-use-of-force-expert-qa-from-stockton-centers-russia-ukraine-conference/>, accessed 1 May 2024.
[189] 'Ukraine War: What Are the Impacts on the World Today?' (International Rescue Committee, 23 August 2022), <https://www.rescue.org/article/ukraine-war-what-are-impacts-world-today > accessed 1 May 2024.
[190] *Ibid.*
[191] *Ibid.*
[192]War of the Future: Drones Playing a Significant Role in the Ukraine War (i24news, 2023) <https://www.i24news.tv/en/news/ukraine-conflict/1677160351-war-of-the-future-drones-playing-a-significant-role-in-the-ukraine-war>, accessed 1 May 2024.
[193]Mariano Zafra, et al, 'How drone combat in Ukraine is changing warfare' (Reuters, 26 March 2024) <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/>, accessed 5 May 2024.

amateur racers and videomaking; however, Ukraine has used them for surveillance and targeting purposes.[194] These drones are usually piloted from the ground and often crash into explosive-laden targets.[195] FPV drones, are equipped with high-resolution cameras that can take pictures and videos up to a range of 20 kilometres.[196] They cannot fly at very high altitudes; the maximum height they can reach is about 120 meters from the ground.[197] According to this technical information, FPV drones can record good-quality images from a short distance on their way and send and save them to a tablet or another device that is connected to it and normally controlled by a soldier.[198] Ukraine usually attaches explosives and mortars to these drones and uses them to shoot down the ground equipment of the Russian army, such as tanks.[199] Because the conflicts in the eastern regions of Ukraine were mostly near residential areas, FPV drones have recorded and transmitted various images of civilians' private spaces, such as their houses.[200]

The other type of drone in widespread deployment by the Ukrainian army was a Turkish-built drone called Bayraktar TB2.[201] This drone is equipped with electro-optical and infrared cameras, enabling high-resolution imaging day and night.[202] Furthermore, these systems can carry signal intelligence payloads that allow them to eavesdrop on and analyse electronic communications in selected regions.[203] They can also be linked to facial recognition application programs and such images of people disseminated.[204] In this regard, a concern was that the use of these drones has led to indiscriminate surveillance of civilians' data from within conflict regions without proper protection and the possibility of misuse of this data that violates human rights.[205]

On the other hand, Russia widely uses different types of surveillance drones as well. One of the drones used mostly by the Russian army is the Iranian Shahed-129 drone, which flies in a medium attitude and is equipped with high-resolution electro-optical cameras for day and night surveillance.[206] Local people in conflict zones claimed that these drones had been seen several times near residential areas, recording images.[207]

---

[194] *Ibid.*
[195] *Ibid.*
[196] *Ibid.*
[197] *Ibid.*
[198] *Ibid.*
[199] John Doe, 'Drones, Russia, and the Ukraine War' (2024) Foreign Policy <https://foreignpolicy.com/2024/04/09/drones-russia-tanks-ukraine-war-fpv-artillery/>, accessed 6 May 2024.
[200] *Ibid.*
[201] Al Jazeera, 'What do we know about Ukraine's use of Turkish Bayraktar drones?' (2024) https://www.aljazeera.com/news/2022/3/11/turkey-drones-use-ukraine > , accessed 20 May 2024.
[202] *Ibid.*
[203] Enes Esen, Engin Büker and Yüksel Akkale, 'The Proliferation of Bayraktar TB2 Drones and Their Risks' (Institute DE, 7 April 2023) <https://www.institude.org/analysis/the-proliferation-of-bayraktar-tb2-drones-and-their-risks>, accessed 20 May 2024.
[204] *Ibid.*
[205] Generally see Office of the United Nations High Commissioner for Human Rights, 'Spyware and surveillance: Threats to privacy and human rights growing UN report' (OHCHR, 14 September 2022) <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>, accessed 24 May 2024.
[206] Michael Knights and Alex Almeida, 'Iranian Drones to Russia: Capabilities and Limitations' (The Washington Institute, 21 November 2022) <https://www.washingtoninstitute.org/policy-analysis/iranian-drones-russia-capabilities-and-limitations>, accessed 24 May 2024.
[207] *Ibid.*

Another UAV Russia uses is the Orlan-10 drones, which have similar capabilities to the Shahed-129 but are more powerful in performing signals intelligence and electronic warfare tasks such as recording communications.[208]

Furthermore, in the occupied parts of Ukraine, including Crimea and Kherson, there is evidence of using surveillance drones for voice recording and eavesdropping on civilians, especially to monitor political discussions between them, which has negative impacts on the right to freedom of expression.[209] Additionally, Russia has used such technologies to prevent children from attending online Ukrainian classes. [210]

Despite the obligations of states to protect civilians' privacy as stipulated in Article 17 of the ICCPR and Article 27 of GC IV, it seems that Russia fails to comply with these obligations. For example, Russian soldiers forcefully entered and looted private residences in Myrnenska and Kherson without justification.[211] Such actions are considered violations because General Comment No. 16 emphasizes that privacy interference must be lawful and non-arbitrary.[212] The soldiers' entry without authorization lacked legal necessity, highlighting their interference as arbitrary and unlawful, which violated Article 8 of the ECHR.[213] Hence, Russia violates these legal norms and does not provide the civilians' privacy that the IHRL requires.

Additionally, due to the lack of regulations regarding data protection in IACs and occupations and the extensive use of drones in the Russia-Ukraine conflict, there are significant challenges to protecting civilians' sensitive data.[214] However, some cases, such as *Klass and others v. Germany*, emphasize justified and proportionate actions in surveillance operations, which Russia's practices fail to meet.[215]

The deployment of new technologies such as surveillance drones to collect information in line with the distinction between civilians and combatants and military and non-military objectives as required under Article 48 of the API seems necessary, especially in times of modern conflicts.[216] However, states and their military commanders must keep in mind that in military and surveillance operations, they must minimize the harm to civilian rights and privacy based on the principle of constant care under Article 57 of AP I,[217] which will be elaborated on in the next chapter.

The use of surveillance drones by Russia and Ukraine during the conflict raises significant legal issues under IHL and IHRL. Under IHL, the principle of distinction in Article 48 of AP I demands that the parties distinguish between civilians and combatants.[218] Nevertheless, the

---

[208] Aleksandre Tsereteli, 'Use of Technologies in the Russia-Ukraine War: Analysis' (2023) Freiheit South Caucasus <https://www.freiheit.org/south-caucasus/use-technologies-russia-ukraine-war>, accessed 10 May 2024.

[209] Bureau of Democracy, Human Rights, and Labor, Country Reports on Human Rights Practices: Ukraine – Russia-Occupied Areas (2022) <https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/ukraine/russia-occupied-areas/>, accessed 10 May 2024.

[210] *Ibid.*

[211] *Ibid.*

[212] *Ibid.*

[213] *Ibid.*

[214] Lubin (n 23), 486-487.

[215] *Klass and Others v. Germany* (n 46), para 50.

[216] Lubin (n 23), 488.

[217] Watt (n 12), 177.

[218] AP I (n 36), art 48: "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between

mentioned drones engaged in recording private residents' data, which can be assessed as a failure to comply with this principle. Additionally, the utilization of drones for monitoring purposes in residential areas without justification signifies a disregard for the precautionary duty outlined in Article 57 of AP I, which is a failure to exercise all practical measures to safeguard civilians from the hazards associated with military activities is evident.[219] Under IHRL, the extensive surveillance, especially the high-resolution imaging, lack clear legal justification and necessary safeguards, rendering these actions arbitrary and unlawful based on Article 17 of the ICCPR.[220]

In conflict situations, the risk of violating civilians' data and privacy rights is high because of the lack of clear regulations.[221] The case of surveillance drones in the Russia-Ukraine war is a limited but clear example that shows that during IACs, civilians' privacy and data protection rights were violated while little legal attention was given to this issue, and this itself provides the groundwork for more widespread violations of these rights with further technological advancements in the future.

4.3 Second Case: Biometric Data Collection in Occupied Territories of Palestine

The occupation of Palestinian territories, including the West Bank and Gaza Strip, by Israel following the six-day conflict in 1967 has led to a significant controversy in international society and numerous issues regarding humanitarian law, human rights, and security.[222] This long occupation has been the subject of many humanitarian debates, including the possibility of genocide, indiscriminate targeting of civilians, torture, violations of the right to freedom of movement, and other human rights.[223]

Similar to the concerns regarding humanitarian issues, civilians' rights to privacy and data protection were also the subject of concern. It is obvious now that Israel is evaluating its new military intelligence technologies in occupied Palestine.[224] Israel, during its years of occupation, has implemented various projects to collect and control a database of civilian populations in occupied territories.[225] For example, 'Unit 8200' is the most famous Israeli military agency in occupied Palestine that collects data.[226] This unit started the biometric collection process by the 'Basel System' in 1999, which was related to collecting biometric data of Palestinian laborers in occupied zones that expanded and progressed over time.[227]

---

civilian objects and military objectives and accordingly shall direct their operations only against military objectives."

[219] Watt (n 12), 178.

[220] ICCPR (n 40), art 17.

[221] Lubin (n 23), 491-492.

[222] Hope O'Dell, 'Israel has occupied Palestinian territories since 1967; UN court considers whether that's legal' (Global Affairs, 20 February 2024) <https://globalaffairs.org/bluemarble/israel-has-occupied-palestinian-territories-1967-un-court-considers-whether-thats-legal>, accessed 15 May 2024.

[223] Amnesty International, 'Israel and Occupied Palestinian Territories 2023' (Amnesty International, 2024) <https://www.amnesty.org/en/location/middle-east-and-north-africa/middle-east/israel-and-occupied-palestinian-territories/report-israel-and-occupied-palestinian-territories/>, accessed 15 May 2024.

[224] Yousef Shehabi (n 117), 90.

[225] *Ibid*, 91-94.

[226] *Ibid*.

[227] Privacy International, 'Biometrics and Counter-Terrorism: Case Study of Israel/Palestine' (2021) 9 <https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israel-palestine> , 11-13, accessed 15 May 2024.

In 2018, Israel added facial recognition technologies to checkpoints in occupied zones.[228] Thus, around 450,000 Palestinians in the West Bank were fingerprinted and photographed, and their data was saved in the database of 'Any Vision' which is the Israeli executive company involved in this project.[229]

Another project that Israel has implemented is the 'Blue Wolf' project, which is based on a smartphone app connected to a database containing photographs of Palestinian inhabitants in occupied zones.[230] To determine the authorization for passage, interrogation, or arrest, a colour-code system is integrated with the facial recognition biometrics of civilians.[231] Additionally, Israel has recently initiated the 'Lavender' project, which pertains to the utilization of AI for target identification.[232] The Defense Force of Israel has claimed that "this system is simply a database whose purpose is to cross-reference intelligence sources."[233] This means that Israel uses its biometric and information database for targeting, which has resulted in the killing of hundreds of civilians.

The widespread implementation of such projects not only affects targeting and distinction rules but also has the potential to have destructive effects on privacy and data protection rights. For instance, in 2014, several officers in 'Unite 8200' stated in a letter that they no longer participated in missions in the West Bank region because of mass surveillance against the civilian population.[234] According to reports, Israeli security forces use collected biometrics to control civilian movements and relationships, collect information about their vulnerabilities, and misuse the data to threaten these civilians and force them to work for Israeli agencies.[235] This highlights the potential misuse of civilians' data and the violation of their privacy rights through different intelligence collection techniques.

Israel has claimed that the ICCPR is not applicable in the occupied territories because the states' human rights obligations are not extraterritorial based on Article 2(1) of the ICCPR.[236] They argued that ICCPR's protections only apply to individuals who are "both physically within its territory and legally subject to its jurisdiction" because they believe that the "and" in Article 2(1) is conjunctive rather than disjunctive.[237] However, as discussed above, based on the ICJ statements,[238] Israel's argument is not acceptable.[239] Furthermore, the Israeli Supreme Court,

---

[228] Amitai Ziv, 'This Israeli Face-recognition Startup Is Secretly Tracking Palestinians' Haaretz (15 July 2019) <https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359 >, accessed 15 May 2024.
[229] Daniel Estrin, 'Face Recognition Lets Palestinians Cross Israeli Check posts Fast, But Raises Concerns' NPR (29 August 2019) <https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>, accessed 18 May 2024.
[230] Yousef Shehabi (n 117), 91.
[231] *Ibid*, 92.
[232] Natasha Karner, 'Israel accused of using AI to target thousands in Gaza, as killer algorithms outpace international law' (The Conversation, 11 April 2024) <https://theconversation.com/israel-accused-of-using-ai-to-target-thousands-in-gaza-as-killer-algorithms-outpace-international-law-227453>, accessed 18 May 2024.
[233] *Ibid.*
[234] Benjamin G Waters, 'An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories' (2019) 50 Geo J Int'l L, 573, 573-575.
[235] *Ibid*, 575.
[236] Human Rights Committee, 'Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant, Fourth Periodic Report of States Parties Due in 2013, Isr.' (UN Doc CCPR/C/ISR/4, 2013), paras 45-49.
[237] *Ibid.*
[238] *Wall Advisory Opinion* (n 19), para 179.
[239] Waters (n 230), 578-579.

also known as the High Court of Justice, has presumed that the ICCPR extends to occupied Palestine, both before and after the ICJ *Wall Advisory Opinion*, which supports the inadmissibility of Israel's argument. It is worth highlighting that Israel maintains this line of argumentation, disregarding the advisory opinion of the ICJ and the stance of the Israeli Supreme Court.[240]

Another argument that Israeli authorities mention is the necessity of security issues in occupied Palestine, which justifies such projects for collecting civilian biometrics.[241] They refer to Article 43 of the Hague regulations, which states, "The occupier shall take all the measures in his power to restore and ensure, as far as possible, public order and safety, while respecting, unless absolutely prevented, the laws in force in the country."[242] Israel also invokes Article 64 of the GC IV, which stresses that:

> "The occupying power may, however, subject the population of the occupied territory to provisions which are essential to enable the occupying power to fulfill its obligations under the present Convention, to maintain the orderly government of the territory, and to ensure the security of the occupying power..."[243]

This argument is strong; the existing regulations do not prohibit the surveillance of civilian populations in occupied territories.[244] Therefore, biometric data collection from civilians *prima facie* appears to be a legitimate security precaution, reminiscent of an occupying power's discretion in selecting such measures.[245] However, the Israeli data collection program extends beyond these justifications, and its use to entrench the occupation breaches GC IV.[246] Moreover, the occupation should be temporary and aim to end as soon as possible, as reflected in the preamble of GC IV and the spirit of the Hague Regulations.[247] Thus, while Israel cites security concerns, using surveillance programs to deepen the occupation violates international regulations.

However, unlike the detailed provisions under the GDPR, such as *the principle of purpose limitation and data storage restrictions*, IHL and IHRL do not offer specific rules or guidelines to regulate the scope and objectives of surveillance in occupied territories.[248] Consequently, this could be considered a gap that fails to protect the privacy and data protection rights of civilians in occupied zones against the threats that originate from biometric and other personal data collection projects.

Additionally, it should be mentioned that some scholars, such as Asaf Lubin, argue that reference to security reasons to justify the mass collection of civilian biometric and personal data and using them for military and non-military purposes is not acceptable in the situation of Palestine.[249] Lubin argues that in long-term occupations, the focus of biometric collection

---

[240] *Ibid.*
[241] Yousef Shehabi (n 117), 104-105.
[242] Hague Convention No IV (n 92), art 43.
[243] GC IV (n 93), art 64.
[244] Yousef Shehabi (n 117), 106.
[245] *Ibid.*
[246] *Ibid.*
[247] Jean S Pictet (ed), Commentary on the Geneva Conventions of 12 August 1949, Volume IV (ICRC 1958), commentary on Article 6, para 60.
[248] Roos (n 149), 15.
[249] Lubin (n 23), 486.

activities is administrative and bureaucratic, not military.[250] Because biometric data is classified as sensitive under data protection law, it necessitates stringent safeguards, including privacy and data protection impact assessments.[251] Consequently, Israel, under international law, is obligated to adhere to data protection principles, guaranteeing the integrity and security of biometric databases as well as providing timely notification to Palestinians in the event of data breaches.[252] Thus, Israel cannot justify this mass surveillance with security issues and should comply with data protection principles and privacy rights enshrined in the laws in force at the time of occupation, which are Jordanian law of 1967 and Egyptian law of 1967, respectively, in the West Bank and Gaza.[253]

However, I affirm that according to the explicit occupation regulations under the Hague regulations and the exceptional conditions in occupied territories, the occupier's activities for biometric data collection could be considered under security and military conditions.[254] Nevertheless, this cannot negate the necessity of the enforcement of laws in force at the time of occupation and the gap in IHL and IHRL for regulating data collection activities in such situations.[255] Moreover, while justification for such surveillance programs could be possible, their compliance with IHL standards remains pivotal. However, analysis shows that Israel's objectives are primarily not oriented only towards security and military imperatives and necessarily do not align with permissible actions under IHL and the rights of the occupied population.[256]

In light of this, the tension between such justifications and IHRL obligations becomes evident. The rules of occupation, which emphasize more on security, potentially are in tension with IHRL's protection of privacy and data.[257] The complexity lies in the challenge of safeguarding security without violating the rights of the occupied population.[258] Thus, while security concerns are valid, any measures taken must adhere to IHL and IHRL principles to avoid compromising human rights in conflict zones.[259]

This example highlights the inherent challenges of protecting data and privacy in occupied territories. The ambiguity in regulations that govern occupiers' responsibility in protecting human rights and the lack of provisions in data protection under IHRL and IHL pose risks to the privacy rights of civilians in occupied zones.

In the next chapter, I will try to answer how it is possible to bridge this gap and what adaptations should be considered in existing IHL and IHRL frameworks regarding data protection and privacy.

---

[250] *Ibid*.
[251] *Ibid*, 487
[252] *Ibid*.
[253] *Ibid*, 488.
[254] Yousef Shehabi (n 117), 105.
[255] *Ibid*, 107-110.
[256] *Ibid.*
[257] *Ibid*, 111-112.
[258] *Ibid*.
[259] Watt (n 12), 179.

5 Bridging Privacy Gaps in Conflict-Affected Areas: Normative Analysis

As elaborated in previous chapters, the deployment of new military technologies such as drones for intelligence gathering and targeting raised concerns in the context of civilians' privacy rights in conflict-affected zones. Protecting data and privacy in such situations becomes more complicated due to the mentioned lack of protection measures under IHL and IHRL for these rights.[260] In this regard, Asaf Lubin states that "there is relatively limited IHL scholarship or ICRC legal opinion around the nature and scope of application of the rights to privacy or data protection in times of armed conflict."[261]

Such substantial gaps in the regulations addressing privacy in conflict-affected zones have the potential to give discretion to a few military members who might not completely recognize the humanitarian implications of their data gathering operations.[262] Furthermore, due to the lack of regulations for privacy protecting obligations, states might potentially prioritize military efficiency over human rights obligations without properly justifying their use of invasive surveillance technologies and applying necessary measures for protecting civilians' privacy. [263]

These concerns have also been recognized by the ICRC as a significant challenge for IHL in the context of contemporary armed conflicts. The ICRC stated that "certain uses of digital technology other than as means and methods of warfare have led to an increase in activities that adversely affect civilian populations."[264] It gives various examples to support this argument, such as reports that mass surveillance of civilians by using new technologies has led to increased concerns and arrests, which put civilians' rights at risk in conflict zones.[265] According to what was discussed in Chapter 3, and these arguments from scholars and the ICRC, the necessity for modifications under IHL and also IHRL to provide better protection for civilians' privacy rights during IACs and occupations becomes more remarkable.

In this chapter, I take steps to answer the main research question by answering this sub-question: What legal adaptations are necessary to address the regulatory and protection gaps concerning the mentioned technologies in conflict-affected zones? The analysis method in this chapter is mainly normative to find normative grounds in IHL and IHRL for proposing reforms to bridge identified gaps, especially in data protection rights in digitalized warfare. Moreover, I will suggest a few recommendations for modifications, specifically under IHL and their possible challenges.

5.1 Normative approach and its basis

The normative approach to legislative reforms in the field of privacy and data protection during IACs and occupations in this research includes an analysis of several ethical and humanitarian principles that guide proposals to clarify 'what regulations ought to be rather than merely what

[260] Lubin (n 23), 474.
[261] *Ibid*, 475.
[262] *Ibid*.
[263] Jakob Kellenberger, 'International Humanitarian Law and Other Legal Regimes: Interplay in Situations of Violence' (ICRC, 4 September 2003), 652 < https://www.icrc.org/eng/assets/files/other/irrc_851_kellenberger.pdf >, accessed 26 May 2024.
[264] ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (Casebook.icrc.org, 2019), section A, paras 7-8, <https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflict-2019>, accessed 10 April 2024.
[265] *Ibid*, paras 109-110.

they are'.[266] In this regard, principles of human dignity, constant care, and precautions in attack will be analysed as the basis of normative suggestions.

5.1.1 Human Dignity

Human dignity is a fundamental principle in IHRL, and many human rights, including privacy, are based on this principle.[267] From a philosophical perspective, human dignity has two dimensions. Initial human dignity means that human status has an absolute inherent value.[268] Initial dignity, as a "constitutive element" of personal identity, exists at all times and distinguishes humans from other creatures.[269]

The second dimension of human dignity, known as 'realized dignity', elaborates on how much human dignity is implemented in the situation of a certain individual.[270] The level of realized dignity depends on humans' relationships with themselves and others, which means that a human being might have a higher or lower degree of recognized dignity in comparison with others.[271]

From a legal perspective, human dignity is one basis of democratic political culture, which is reflected in various legal frameworks.[272] For example, at the international level, the preamble of the UN Charter [273] and the UDHR[274] have referred to the initial dimension of human dignity for legislating. Human dignity, also in the context of theoretical approaches to international law, has been considered the basis of normative approaches. For instance, the New Haven School of International Law normatively analyses international regulations based on global standards of human dignity.[275] The scholars in this school argue that the law is a tool intended to promote human dignity and global public order.[276]

The fact that the theoretical basis of privacy and data protection rights is human dignity could be supported by different sources. For instance, Article 11 of the American Convention on Human Rights connects privacy with dignity when, it states that "everyone has the right to have his honour respected and his dignity recognized."[277] Moreover, in the case of *Kucera v. Slovakia*, the ECtHR referred to safeguarding human dignity against abuses of power in interpreting the right to privacy.[278] Similarly, Article 17 of the ICCPR on protecting privacy notes the significance of human dignity by highlighting "his honour and reputation."[279] GDPR, also regarding data protection, notes that "Member States should incorporate certain safeguards

---

[266] Eliav Lieblich, 'How to Do Research in International Law? A Basic Guide for Beginners' (2021) 62 Harvard Journal of International Law, 46. 46-47.
[267] Lubin (n 23), 480.
[268] Petra Kleindienst and Matevž Tomšič, 'Human Dignity as the Foundation of Democratic Political Culture: Legal and Philosophical Perspective' (2022) 18(2) Law, Culture and the Humanities 385, 388-389.
[269] *Ibid*, 390.
[270] *Ibid*.
[271] *Ibid*.
[272] *Ibid*, 391.
[273] United Nations Charter (signed 26 June 1945, entered into force 24 October 1945) 59 Stat 1031, UNTS 993, Preamble, para 2
[274] UDHR (n 39), art 1.
[275] Molly Land, 'Reflections on the New Haven School' (2014) 58(4) NYLS Law Review 919, 920-922.
[276] *Ibid*.
[277] American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) OAS Treaty Series No 36, art 11.
[278] *Kucera v. Slovakia* App No 48666/99 (ECtHR, 17 July 2007), para 122.
[279] ICCPR (n 40), art 17.

to protect data subjects' human dignity."[280] As elaborated, IHL also uses the theory of human dignity in protecting civilians in times of conflict and occupation, such as prohibiting superfluous injuries to enemy combatants in Article 35(2) of AP I.[281]

Hence, the principle of human dignity, which is embedded in IHL and IHRL, could justify reforming existing rules to better protect civilian privacy and, especially, their data against threats originating from surveillance technologies.[282]

Nevertheless, the increasing number of surveillance drones and data mining technologies raise issues of human dignity. Such technologies often violate individuals' privacy by continuously monitoring them without their consent, creating an environment of suspicion that might result in stripping civilians of their sense of personal space and autonomy.[283] The mentioned practices have the potential to contradict the principle of human dignity as they could diminish civilians in conflict-affected areas as data sources, undermining their right to privacy.[284]

Some legislative measures can be taken to preserve human dignity, for example, restricting the use of surveillance drones to specific circumstances and granting transparency in data collection, as exemplified by the GDPR. Impingement on human dignity is at the center of the application *Big Brother Watch v. UK*, in which the ECtHR ruled that searching through data obtained through bulk interception constituted a violation of privacy.[285] The court highlighted how human dignity can be affected by indiscriminate massive database recording without sufficient safeguards to protect against disproportionate interference, and it notes that states should seek to implement an effective system of oversight and redress to mitigate abuses of power. [286]

Therefore, in conflict-affected areas, explicit obligations should be imposed on states and their forces to uphold privacy and provide remedies for violations, thereby enhancing human rights in conflict-affected zones and the accountability of perpetrators.[287] Thus, human dignity can be improved by protecting privacy rights in the face of technological incursions.

5.1.2 Constant Care and Precautions

Another ground for bridging the normative gap to protect privacy rights in conflict situations is the principle of constant care, which is enshrined in Article 57(1) of AP I. Commanders and troops must take into account the effects of their operations on civilian populations and implement measures to mitigate these consequences.[288] According to the Tallinn Manual 2.0, the constant care duty also applies to the states' cyber attacks.[289] Moreover, this duty is

[280] GDPR (n 54), art 82(2).
[281] AP I (n 36), art 35(2).
[282] Lubin (n 23), 481.
[283] *Ibid*.
[284] *Ibid*.
[285] *Big Brother Watch and Others v. United Kingdom* App nos 58170/13, 62322/14, 24960/15 ECtHR [2021], para 387.
[286] *Ibid*, para 463.
[287] Watt (n 12), 179.
[288] *Ibid*, 176.
[289] Michael N Schmitt and Liis Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) Rule 114, paras 4-5.

'constant' which means this situational awareness is essential in all stages of military operations, such as during the preparation stage and even after active hostilities.[290]

Based on this argument, the application of constant care in the context of surveillance and intelligence gathering is logical for adjusting humanitarian rules to protect data and privacy rights.[291] If constant care is applicable during cyber operations, it makes sense that it should be applied during intelligence gathering by using drones and biometric collection because these are informational operations to support military operations.[292]

Furthermore, it may seem that the drafters of AP I considered the physical harm to civilians, including deaths and injuries, concerning "attack" in Article 57.[293] However, it cannot be denied that using new military technologies has also had negative effects on the non-physical rights of civilians, which especially becomes crucial as militaries increasingly rely on technological tools such as machine learning and AI to enhance decision-making processes.[294] Therefore, the duty of constant care should be used to improve normative legislation against arbitrary interference with civilians' privacy, including the right to autonomy and dignity.

Moreover, the customary rule of precaution under Rule No. 115, which derives from the principle of constant care, also emphasizes "all feasible precautions when selecting a means and method of attack to minimize incidental civilian casualties."[295] This rule puts positive obligations on states to be aware of their means and methods in their operations.[296] Likewise, it could support this argument that such responsibility encompasses the need for states to be mindful of their selection of surveillance programs and strategies while also safeguarding human rights, including privacy.[297]

However, using surveillance drones and collecting biometric data, for example, could undermine the principle of constant care because it sometimes makes it harder to minimize harm to civilians.[298] Drones initially cannot distinguish between combatants and non-combatants and cannot react appropriately to complex situations, as seen in attacking civilians in conflicts in Yemen and Syria.[299]

Biometric data collection is also often used without informed consent or robust safeguards that raise the risks of abuse, as seen in the Palestine case.[300] Thus, the deployment of such technologies, without oversight and strict instructions for use during military operations, could potentially undermine the constant care and precautions.

Therefore, maintenance of constant care principles in technological utilization would improve the protection of civilians in conflicts and occupations. Providing stringent guidelines to ensure

---

[290] *Ibid*, para 5.
[291] Watt (n 12), 176-178.
[292] *Ibid.*
[293] *Ibid*, 177.
[294] *Ibid.*
[295] Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law: Volume I: Rules (CUP 2005) Rule 115.
[296] See Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia (13 June 2000) <http://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal>, accessed 25 May 2024, para 50.
[297] Watt (n 12), 178-179.
[298] *Ibid.*
[299] *Ibid.*
[300] Yousef Shehabi, (n 117), 109-112.

the proportionality of surveillance and its respect for privacy rights are part of these crucial safeguards.

5.1.3 Ethical Considerations in Decision Making

As stated before, achieving a balance between human rights, ethical concerns, and security issues is a complicated subject that requires a complete investigation of social, philosophical, and legal aspects, which is beyond the scope of this thesis. However, shortly I will point out a few ethical considerations as examples that could be the basis for normative adaptations.

Similar to IHL, the ethical norms require that intelligence gatherings be periodically reviewed to see if they are proportionate and necessary.[301] This scrutiny serves to analyse whether less invasive measures could achieve the same security goals and prevent surveillance measures from becoming arbitrary or excessively invasive of privacy.[302] For example, in the occupied territories, normal ID cards can be used instead of face-recognition technologies at checkpoints.[303] In the context of warfare, from the perspective of utilitarian ethics, it is important to define what can be acknowledged as being ethical by providing the most good for most people and the least harm for non-combatants.[304] Thus, states should conduct assessments to evaluate the potential risks of using surveillance drones and data mining technologies in military operations, such as privacy invasions and similar violations.[305]

Moreover, the approach of the duty framework, which is based on deontological ethics, determines the ethical status of the action regarding its responsiveness to the rules that provide guidance in resolving the case and the subsequent consequences of such practice.[306] The principle of human dignity also aligns with this claim because it safeguards fundamental human rights.[307] In this regard, states should ensure strict adherence to IHRL and IHL when implementing surveillance measures, considering the impact on civilian rights in light of security threats.[308]

Additionally, states collecting civilians' personal data, even during conflicts or occupations, should consider that civilians ethically have the right to understand how it will be used and how its confidentiality, integrity, and accuracy will be protected.[309] Thus, states should express the purpose of such collections clearly in their policies for data collection.[310] Moreover, authorities are ethically required to provide notification in case of a violation or misuse of the

---

[301] Daniel J. Power, Ciara Heavin and Yvonne O'Connor, 'Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide' (2021) 4(2) Journal of Business Analytics 155, 156.
[302] *Ibid*, 158.
[303] Yousef Shehabi (n 117), 106.
[304] John W. Lango, The Ethics of Armed Conflict: A Cosmopolitan Just War Theory (Edinburgh University Press 2014), 3-5.
[305] Lubin (n 23), 485.
[306] Power, Heavin and O'Connor (n 301), 159.
[307] Kleindienst and Tomšič (n 268), 389.
[308] United Nations Office on Drugs and Crime, 'Privacy, Intelligence Gathering and the Use of Surveillance in Armed Conflict' (Education for Justice, SHERLOC) <https://sherloc.unodc.org/cld/en/education/tertiary/terrorism/module-12/key-issues/privacy-intelligence-gathering-in-armed-conflict.html > accessed 30 May 2024.
[309] M Haider, 'An Ethical Approach to Data Privacy Protection' (2016) 6 ISACA Journal <https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/an-ethical-approach-to-data-privacy-protection>, accessed 1 June 2024.
[310] *Ibid.*

collected sensitive data.[311] Such ethical considerations have the potential to drive normative changes that better protect privacy rights during conflicts and occupations.

5.2 Recommendations and Challenges

Based on the given normative bases, to bridge existing privacy gaps in conflict-affected areas, it is critical to recommend particular measures addressing privacy, especially data protection rights in IHL and IHRL.

The primary measurement is to ratify the incorporation of the right to privacy and data protection into the GCs and APs. This could include drafting specific articles that clearly define the limitations and standards for mass surveillance and data collection of civilians in IACs and occupations similar to the protection that was given to their physical bodies.[312] Such provisions should guarantee the military forces' compliance with the minimization principle regulating any data collection activities and ensuring that data collection operations are strictly proportional under the strict supervision of commanders.[313]

However, as Yousef Shehabi states, the current lack of clear rights to privacy and data protection under the IHL is unlikely to change soon and will face different challenges in the revision process.[314] It is difficult to bring states to an agreement on changes to IHL rules or add an AP for protecting human rights in conflicts because states are likely to oppose changes that would limit military activities, as there is no customary consensus on protecting privacy rights at this moment.[315] However, this is not impossible and might happen again with international cooperation between states, NGOs, and international organizations (IOs), like what happened in the adoption of the current APs.[316]

Another recommendation is to clarify data protection rights within the IHRL framework as a complementary tool for IHL. Defining basic protective measures such as transparency, limitation of data collection, and the right to be informed about data collections could potentially improve the privacy situation during conflicts and occupations.[317] GDPR could be a model for adjusting IHRL rules.[318] Considering IHRL evolves more dynamically through international bodies, such as the human rights committee, it could adapt to new human rights issues.[319] For example, new UNGA resolutions on privacy suggesting remedies for violations of data protection rights highlight these potentials in IHRL.[320]

However, even if such changes happen, they could be effective in the context of conflicts and occupations when it is accepted by all states that IHRL is applicable in conflicts and occupations. Furthermore, they should agree that IHL must be interpreted in line with IHRL,

---

[311] Lubin (n 23), 491.
[312] Watt (n 12), 180.
[313] *Ibid.*
[314] Yousef Shehabi, (n 117), 111-112.
[315] *Ibid.*
[316] Watt (n 12), 180.
[317]Tal Mimran and Yuval Shany, 'Privacy in Article 36 Reviews of New Technologies: Integrating Privacy Concerns in the Development and Introduction of New Military or Dual-Use Technologies' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022) 29, 39-40.
[318] Lubin (n 23), 490.
[319] Françoise J. Hampson, 'The Relationship Between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body' (2008) 90(871) International Review of the Red Cross 549, 552-554.
[320] See UNGA Res 69/166 'The Right to Privacy in the Digital Age' (10 February 2015) UN Doc A/RES/69/166.

all human rights obligations must be fulfilled, and even restricting privacy rights in certain conditions must be limited and within the framework of IHRL.[321] Meanwhile, as mentioned, states, such as Israel dispute that ICCPR is applicable in occupied Palestine.[322]

Additionally, developing international guidelines for the use of drones and new technologies such as AI for surveillance and intelligence gathering during IACs and occupations could enhance civilians' privacy.[323] For instance, the ECtHR's requirements in the *Big Brother Watch v. United Kingdom* judgment can be a template for the military using UAVs for intelligence purposes.[324] In this case, the ECtHR suggests eight guarantees for protecting privacy during broad surveillance operations, such as imposing limits on the duration of the interception, the limited storage of the intercepted material, and collecting data, which could be a model for developing international guidelines.[325]

The constantly evolving surveillance technologies present a challenge in maintaining timely guidelines.[326] However, it is essential to establish flexible international frameworks that can be adjusted to align with domestic regulations in protecting privacy.[327] Additionally, the establishment of supervisory agencies with the responsibility of enforcing privacy and data protection in domestic rules, conducting investigations into alleged infringements, and prescribing necessary corrective actions is crucial.[328]

Moreover, it should be noted that the role of the ICRC in bridging this gap is crucial. In this regard, Christopher Kuner argues that if the ICRC provides data protection guidelines, "it could gradually crystallize international law."[329] This thesis focuses on the proposal that states should strengthen international data protection and privacy laws during conflicts. Given the ICRC's role as the main organization responsible for promoting IHL, if it cannot acknowledge data protection as a human right openly, it becomes questionable to expect states to do so.[330] The UN and ICRC are exemplary models and responsible for setting a positive precedent in advancing legislation that promotes expanded privacy rights and safeguards humanitarian data.[331] To further promote the agenda of conflict-time privacy and data protection, the ICRC and other IOs should reiterate their legal role to uphold the expanding international rule of law in this field.[332]

Finally, states can take several actionable steps to align their conduct with human rights obligations. For instance, they can adopt less extensive interpretations of the principles of proportionality and necessity to minimize intrusive surveillance on civilians in conflicts and

---

[321] Lubin (n 23), 478-479.
[322] Human Rights Committee, 'Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant (n 236), para 45-49.
[323] Watt (n 12), 178.
[324] *Ibid.*
[325] *Big Brother Watch and Others v. United Kingdom* (n 285), para 361.
[326] Lubin (n 23), 491-492.
[327] *Ibid.*
[328] *Ibid.*
[329] Christopher Kuner, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Oxford University Press 2019) 112, 131.
[330] Asaf Lubin, 'Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study' in R. Buchan and A. Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022), 259.
[331] *Ibid.*
[332] *Ibid.*

occupations, as Sassòli argues that restrained interpretations of these principles are crucial for upholding humanitarian values in modern warfare.[333]

Furthermore, states can give higher priority to privacy as a human right in conflict-affected zones to contribute to the progressive development of IHL and IHRL norms. For example, Germany's implementation of stringent data protection regulations in counter-terrorism operations highlights that states can practically use less extensive interpretations of security.[334]

Consequently, the tension between military necessity and human rights obligations is recognizable. However, states, by wishfully accepting a less ambitious interpretation, can promote the rights' compliance culture in conflict circumstances, possibly forming the overall international attitude in the long term.

In the next chapter, I will conclude the findings of this thesis.

6 Conclusion

In this thesis, I sought to gain a better understanding of how existing IHL and IHRL frameworks can change to protect civilians' rights to privacy and data protection more effectively in the context of IACs and occupations, particularly considering the use of surveillance drones and biometric collection technologies. To conclude, I consolidate how the main findings of this thesis answer my main research question.

The main findings of this research highlight a critical gap in existing IHL and IHRL concerning data and privacy rights. Although both of these complementary frameworks aim to enhance the protection of human rights in conflict-affected areas, they lack specific provisions addressing the privacy implications of modern surveillance technologies. This normative gap, especially regarding data protection, has made room for potential abuses and unjustified limitations in civilians' privacy and data protection rights through bulk surveillance in combat zones and occupied territories. Through evaluating IHL and IHRL related to data and privacy rights and surveillance technologies in the Russia-Ukraine conflict and occupied Palestine, I revealed several key insights.

Firstly, the right to privacy is a fundamental human right recognized by IHRL instruments such as ICCPR and UDHR, which have roots in the principle of human dignity. Data protection is closely related to privacy but deals with regulating personal data processing to prevent unauthorized access and misuse. Therefore, privacy and data protection are two distinct human rights; however, under the IHRL, data protection has yet to be recognized.

Secondly, the analysis highlighted that although IHL and IHRL have different scopes and applications, based on the ICJ statements and scholars' arguments, these are complementary tools for protecting human rights, especially for non-combatants in conflict situations. However, even privacy protections in IHRL could not protect civilians' data and privacy in conflict-affected areas concerning new surveillance technologies. The comparison with newer regulations such as GDPR highlighted the inadequacies of IHL and IHRL, especially regarding the implementation of state obligations and emphasizing the need for adopting more stringent

[333] Marco Sassòli, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare (Edward Elgar Publishing 2019), 123-125.

[334] Bundesdatenschutzgesetz (Federal Data Protection Act of Germany, 2019) s 15.

data protection measures to better protect civilians' digital privacy during conflicts and occupations.

Thirdly, examining cases of the deployment of surveillance drones in the Russia-Ukraine conflict and biometrics collection in occupied Palestine stressed that the use of such surveillance technologies has increased in recent decades and posed concerns about the extent of data collected and the purposes for which it is used, which complicates the protection of privacy rights more.

Finally, to address the regulatory gap, I proposed several adaptations based on human dignity, the principle of constant care, and a few ethical considerations. These consist of explicit privacy and data protection provisions in IHL and IHRL, providing robust supervising mechanisms to ensure states' compliance with these enhanced regulations, strengthening international cooperation on practices for privacy protection in conflict zones, and developing guidelines that minimize data collection and mitigate privacy risks.

Evaluating the main findings of this thesis has some implications for public international law. Firstly, protecting data rights and digital privacy during and after conflicts is an evolving field within international law that requires attention, especially under IHL. The inclusion of privacy safeguards can establish a precedent for other nascent technologies, guaranteeing that progress in warfare does not surpass the legal structures intended to safeguard human rights. This thesis also emphasizes the importance of a dynamic approach to international law that can adapt to technological innovations and their impact on privacy rights.

Moreover, the revisions I recommended can influence international norms and state practices to improve the implementation of strict data protection measures in conflict-affected areas. Additionally, this research contributes to the broader discourse related to the balance between state security policies and human rights.

In conclusion, this thesis highlights the critical necessity for adjustments in regulations governing conflicts and occupation situations to bridge the normative gaps in IHL and IHRL addressing privacy and civilians' data. The international community might protect these rights in a better way by implementing recommendations. This study also provided a foundation for advancing legal frameworks for data and privacy protection in current and future IACs and occupations.

Bibliography

1. Primary Sources

a. Regulations, Conventions, Agreements, and Treaties

United Nations Charter (signed 26 June 1945, entered into force 24 October 1945) 59 Stat 1031, UNTS 993 Preamble.

Universal Declaration of Human Rights (UDHR) (adopted 10 December 1948 UNGA Res 217 A(III)).

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31.

Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85.

Geneva Convention relative to the Treatment of Prisoners of War (Third Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.

Geneva Convention relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention) (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

Hague Convention No. IV Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land (adopted 18 October 1907, entered into force 26 January 1910) 36 Stat 2227 TS No 539.

International Covenant on Civil and Political Rights (ICCPR) (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) OAS Treaty Series No 36.

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) OAS Treaty Series No 36.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108, 1981).

Charter of Fundamental Rights of the European Union (2000/C) 364/01.

General Data Protection Regulation (GDPR), 2016/679 of 27 April 2016, OJ L 119/1.

Bundesdatenschutzgesetz (Federal Data Protection Act of Germany, 2019) s 15.

b. Cases and Advisory Opinions

Klass and Others v. Germany (App no 5029/71) [1978] 2 EHRR 214.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.

Z v. Finland [1997] ECtHR 10.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 136.

Weber and Saravia v. Germany (App no 54934/00) [2006] ECtHR, 46 EHRR SE5.

Kucera v. Slovakia App no 48666/99 [2007], ECtHR.

Hassan v. United Kingdom ECHR 29750/09, [2014] 38 BHRC 358, [2014] ECtHR 993.

Al-Skeini and Others v. United Kingdom [2011] ECtHR 1093.

Big Brother Watch and Others v. United Kingdom [2018] ECtHR 722.

Google LLC v. CNIL (Case C-507/17), [2019] ECLI:EU:C:2019:772.

2. Literature

Albakjaji Mohamad and Almarzoqi Reem, 'The Impact of Digital Technology on International Relations: The Case of the War between Russia and Ukraine' (2023) 2 Access to Justice in Eastern Europe 8 (Hein Online), 8-24.

Benvenisti Eyal, 'Human Dignity in Combat: The Duty to Spare Enemy Civilians' (2006) 39(2) Israel Law Review, 81.

Bertino Elisa and Martino Lorenzo, 'Privacy and Security in the European Union: User Rights and Enforcement' (2019) 15 Journal of Cybersecurity, 145.

Clapham Andrew, 'Human Rights in Armed Conflict: Metaphors Maxims and the Move to Interoperability' (2018) 12 Journal of Human Rights and International Legal Discourse, 9-22.

Clarke Roger, 'What Drones Inherit from Their Ancestors' (2014) 30 Computer Law and Security Review, 247.

Crawford Emily and Pert Alison, International Humanitarian Law, 2nd edn, Cambridge University Press (2020), chapters 1-5.

Fortin Katharine, 'The Relationship Between International Human Rights Law and International Humanitarian Law: Taking Stock at the End of 2022?' (2022) 40(4) Netherlands Quarterly of Human Rights, 343-353.

Hampson Françoise J, 'The Relationship Between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body' (2008) 90(871) International Review of the Red Cross, 549.

Handel Ariel, 'Exclusionary Surveillance and Spatial Uncertainty in the Occupied Palestinian Territories', in Elia Zureik, David Lyon, and Yasmeen Abu-Laban (eds), Surveillance and Control in Israel/Palestine: Population, Territory and Power (2010), 259.

Heyns Christof, Akande Dapo, Hill-Cawthorne Lawrence, and Chengeta Thompson, 'The International Law Framework Regulating the Use of Armed Drones' (2016) 65(4) International & Comparative Law Quarterly, 791-827.

Kittichaisaree Kriangsak, Public International Law of Cyberspace, 1st ed, Springer International Publishing (2017), chapter 3.

Kleindienst Petra and Tomšič Matevž, 'Human Dignity as the Foundation of Democratic Political Culture: Legal and Philosophical Perspective' (2022) 18(2) Law, Culture and the Humanities, 385.

Kuner Christopher, 'The GDPR: Implementation and International Implications' (2019) 25 International Data Privacy Law, 7.

Kuner Christopher, 'The Internet and the Global Reach of EU Law' in Marise Cremona and Joanne Scott (eds), EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law (Oxford University Press 2019), 112.

Land Molly, 'Reflections on the New Haven School' (2014) 58(4) NYLS Law Review, 919.

Lango John W, The Ethics of Armed Conflict: A Cosmopolitan Just War Theory, Edinburgh University Press (2014), 1.

Lieblich Eliav, 'How to Do Research in International Law? A Basic Guide for Beginners' (2021) 62 Harvard Journal of International Law, 46.

Lubin Asaf, '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 (2022), 463.

Lubin Asaf, 'Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study' in R Buchan and A Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022), 259.

Marmor Andrei, 'What Is the Right to Privacy?' (2015) 43 Philosophy & Public Affairs, 3.

Mimran Tal and Shany Yuval, 'Privacy in Article 36 Reviews of New Technologies: Integrating Privacy Concerns in the Development and Introduction of New Military or Dual-Use Technologies' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022), 29.

O'Connell Mary Ellen, 'Data Privacy Rights: The Same in War and Peace' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict NATO CCDCOE Publications (2022), 12.

Pope Carra, 'Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data' (2018) 26 Journal of Law and Policy, 769.

Pomson Ori, '‘Objects’? The Legal Status of Computer Data under International Humanitarian Law' (2023) 28(2) Journal of Conflict and Security Law, 349.

Power Daniel J, Heavin Ciara, and O’Connor Yvonne, 'Balancing Privacy Rights and Surveillance Analytics: A Decision Process Guide' (2021) 4(2) Journal of Business Analytics, 155.

Rengel Alexandra, Privacy in the 21st Century BRILL, Boston (2013), chapter 4

Roos Anel, 'Data Protection Principles under the GDPR and the POPI Act: A Comparison' (2023) 86 Hedendaagse Romeins-Hollandse Reg, 1.

Sassòli Marco, International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare Edward Elgar Publishing (2019), 1.

Schabas William, 'Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum' (2007) 40(2) Israel Law Review, 592.

Shehabi Omar Yousef, 'Digital Privacy and Data Protection in Military Occupation' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict (2022), 87.

Tzanou Maria, 'Data Protection as a Fundamental Right Next to Privacy? “Reconstructing” a Not So New Right' (2013) 3(2) International Data Privacy Law, 88.

Wagner Markus, 'Unmanned Aerial Vehicles' in Anne Peters and Rüdiger Wolfrum (eds), Max Planck Encyclopedia of Public International Law, Oxford University Press, (2014), 2.

Waters Benjamin G, 'An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories' (2019) 50 Georgetown Journal of International Law, 573.

Watt Eliza, 'The Principle of Constant Care Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts' in Russell Buchan and Asaf Lubin (eds), The Rights to Privacy and Data Protection in Times of Armed Conflict, NATO CCDCOE Publications (2022), 157.

Wingo Harry, 'Set Your Drones to Stun: Using Cyber-Secure Quadcopters to Disrupt Active Shooters' (2018) 17(2) Journal of Information Warfare, 54.

3. UN and ICRC Reports

Human Rights Careers, 'Definitions: What is Human Dignity?' (Human Rights Careers) <https://www.humanrightscareers.com/issues/definitions-what-is-human-dignity/> , accessed 19 April 2024.

Human Rights Committee, 'General Comment No. 16: Article 17 (The Right to Privacy) The Right to Respect of Privacy Family Home and Correspondence and Protection of Honour and Reputation' (8 April 1988) UN Doc CCPR/C/GC/16.

Human Rights Committee, 'General Comment No. 29: Article 4 (Derogations during a State of Emergency)' (31 August 2001) UN Doc CCPR/C/21/Rev.1/Add.11, para 3.

Human Rights Committee, 'General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant' (26 May 2004) UN Doc CCPR/C/21/Rev.1/Add.13.

Human Rights Watch, 'A Threshold Crossed: Israeli Authorities and the Crimes of Apartheid and Persecution' (2021) 76 <https://www.hrw.org/report/2021/04/27/threshold-crossed/israeli-authorities-and-crimes-apartheid-and-persecution> , accessed 17 April 2024.

International Committee of the Red Cross, 'Strengthening Legal Protection for Persons Deprived of their Liberty in Relation to Non-International Armed Conflict: Regional Consultations 2012–13' (2013), 5 <https://www.icrc.org/en/doc/assets/files/2013/strengthening-legal-protection-detention-consultations-2012-2013-icrc.pdf> , accessed 4 May 2024.

International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (Casebook.icrc.org, 2019), section A, paras 7-8, <https://casebook.icrc.org/case-study/icrc-international-humanitarian-law-and-challenges-contemporary-armed-conflict-2019 > , accessed 10 April 2024.

International Committee of the Red Cross (ICRC), 'Rule 15: Precautions in Attack' Customary International Humanitarian Law Database (ICRC 2005) <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule15 >, accessed 1 May 2024.

Jean-Marie Henckaerts and Louise Doswald-Beck (eds), Customary International Humanitarian Law: Volume I: Rules (CUP 2005) Rule 115.

Jakob Kellenberger, 'International Humanitarian Law and Other Legal Regimes: Interplay in Situations of Violence' (ICRC, 4 September 2003), 652 <https://www.icrc.org/eng/assets/files/other/irrc_851_kellenberger.pdf>, accessed 26 May 2024.

Michael N Schmitt and Liis Vihul (eds), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (CUP 2017) Rule 114, paras 4-5.

Office of the United Nations High Commissioner for Human Rights, 'Spyware and Surveillance: Threats to Privacy and Human Rights Growing - UN Report' (OHCHR, 14 September 2022) <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report> , accessed 24 May 2024.

Philip Alston (Special Rapporteur), 'Report on Extrajudicial, Summary or Arbitrary Executions' (2010) UN Doc A/HRC/14/24/Add.6, para 1.

UNGA Res 69/166 'The Right to Privacy in the Digital Age' (10 February 2015) UN Doc A/RES/69/166.

UNGA, 'Guidelines for the Regulation of Computerized Personnel Data Files' Res 45/95 (14 December 1990) UN Doc A/RES/45/95, 45th sess, 1990-1991, para 4.

UNECE, Conference of European Statisticians Statistical Standards and Studies – No. 53, 'Terminology on Statistical Metadata' (Geneva, 2000), 42 <https://unece.org/DAM/stats/publications/53metadaterminology.pdf> , accessed 1 May 2024.

United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide (2020) <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> , accessed 1 May 2024.

4. Web-Pages and Others

Aleksandre Tsereteli, 'Use of Technologies in the Russia-Ukraine War: Analysis' (2023) Freiheit South Caucasus <https://www.freiheit.org/south-caucasus/use-technologies-russia-ukraine-war>, accessed 10 May 2024.

Alex Hern, 'Facebook translates "good morning" into "attack them", leading to arrest' (The Guardian, 24 October 2017) <https://www.theguardian.com/technology/2017/oct/24/facebook-palestine-israel-translates-good-morning-attack-them-arrest>, accessed 10 April 2024.

Al Jazeera, 'What do we know about Ukraine's use of Turkish Bayraktar drones?' (2024) <https://www.aljazeera.com/news/2022/3/11/turkey-drones-use-ukraine>, accessed 20 May 2024.

Amnesty International, 'Israel and Occupied Palestinian Territories 2023' (Amnesty International, 2024) <https://www.amnesty.org/en/location/middle-east-and-north-africa/middle-east/israel-and-occupied-palestinian-territories/report-israel-and-occupied-palestinian-territories/>, accessed 15 May 2024.

Amitai Ziv, 'This Israeli Face-recognition Startup Is Secretly Tracking Palestinians' Haaretz (15 July 2019) <https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359>, accessed 15 May 2024.

Brian Pickle, 'Data Definition' (13 December 2022) <https://techterms.com/definition/data#google_vignette>, accessed 1 May 2024.

Bureau of Democracy, Human Rights, and Labor, 'Country Reports on Human Rights Practices: Ukraine – Russia-Occupied Areas' (2022) <https://www.state.gov/reports/2022-country-reports-on-human-rights-practices/ukraine/russia-occupied-areas/>, accessed 10 May 2024.

Council of Europe, 'Drones and Targeted Killing: The Need to Uphold Human Rights and International Law' Doc No 13731 (2015), para 18.

Daniel Estrin, 'Face Recognition Lets Palestinians Cross Israeli Check posts Fast But Raises Concerns' NPR (29 August 2019) <https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>, accessed 30 April 2024.

Dominika Kunertova, 'Drones have boots: Learning from Russia's war in Ukraine' (2023) 44(4) Contemporary Security Policy 576-591.

Doe, John, 'Drones, Russia, and the Ukraine War' (Foreign Policy, 9 April 2024) <https://foreignpolicy.com/2024/04/09/drones-russia-tanks-ukraine-war-fpv-artillery/>, accessed 6 May 2024.
Enes Esen, Engin Büker and Yüksel Akkale, 'The Proliferation of Bayraktar TB2 Drones and Their Risks' (Institute DE, 7 April 2023) <https://www.institude.org/analysis/the-proliferation-of-bayraktar-tb2-drones-and-their-risks>, accessed 20 May 2024.

Estrin, Daniel, 'Face Recognition Lets Palestinians Cross Israeli Check posts Fast But Raises Concerns' NPR (29 August 2019) <https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc>, accessed 30 April 2024.

European Council on Foreign Relations (ECFR), 'Drones in Ukraine and Beyond: Everything You Need to Know' (11 August 2023) <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>, accessed 30 April 2024.

Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia (13 June 2000) <http://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal>, accessed 25 May 2024.

Hope O'Dell, 'Israel has occupied Palestinian territories since 1967; UN court considers whether that's legal' (Global Affairs, 20 February 2024) <https://globalaffairs.org/bluemarble/israel-has-occupied-palestinian-territories-1967-un-court-considers-whether-thats-legal>, accessed 15 May 2024.

Mariano Zafra, et al, 'How drone combat in Ukraine is changing warfare' (Reuters, 26 March 2024) <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/>, accessed 5 May 2024.

Matt Burgess, 'Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory' (Wired, 27 February 2022) <https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/>, accessed 12 April 2024.

Michael Knights and Alex Almeida, 'Iranian Drones to Russia: Capabilities and Limitations' (The Washington Institute, 21 November 2022) <https://www.washingtoninstitute.org/policy-analysis/iranian-drones-russia-capabilities-and-limitations>, accessed 24 May 2024.

Natasha Karner, 'Israel accused of using AI to target thousands in Gaza, as killer algorithms outpace international law' (The Conversation, 11 April 2024) <https://theconversation.com/israel-accused-of-using-ai-to-target-thousands-in-gaza-as-killer-algorithms-outpace-international-law-227453>, accessed 18 May 2024.

Nayef, Omer, 'The Impact of Drone Warfare on International Humanitarian Law' (Just Security, 1 February 2023) <https://www.justsecurity.org/84311/the-impact-of-drone-warfare-on-international-humanitarian-law/> , accessed 6 May 2024.

Peter Bergen et al., 'World of Drones' New America (30 July 2020) <https://www.newamerica.org/international-security/reports/world-drones/>, accessed 15 May 2024.

Remarks by President Biden on the End of the War in Afghanistan, The White House (31 August 2021) <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/08/31/remarks-by-president-biden-on-the-end-of-the-war-in-afghanistan/>, accessed 15 May 2024.

Rina Chandran, 'Afghans Scramble to Delete Digital History, Evade Biometrics' (Reuters, 17 August 2021) <https://www.reuters.com/article/afghanistan-tech-conflict/afghans-scramble-to-delete-digitalhistory-evade-biometrics-idUSL8N2PO1FH>, accessed 15 April 2024.

Thom Shanker, 'To Track Militants, US Has System That Never Forgets a Face' (New York Times, 13 July 2011) <https://www.nytimes.com/2011/07/14/world/asia/14identity.html>, accessed 10 April 2024.

Ulrike Franke, 'Drones in Ukraine and Beyond: Everything You Need to Know' (European Council on Foreign Relations, 11 August 2023) <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>, accessed 30 April 2024.

'Ukraine War: What Are the Impacts on the World Today?' (International Rescue Committee, 23 August 2022) <https://www.rescue.org/article/ukraine-war-what-are-impacts-world-today>, accessed 1 May 2024.

United Nations Office on Drugs and Crime, 'Privacy, Intelligence Gathering and the Use of Surveillance in Armed Conflict' (Education for Justice, SHERLOC) <https://sherloc.unodc.org/cld/en/education/tertiary/terrorism/module-12/key-issues/privacy-intelligence-gathering-in-armed-conflict.html>, accessed 30 May 2024.

W. Casey Biggerstaff, 'Can Aid or Assistance Be a Use of Force?: Expert Q&A from Stockton Centre’s Russia-Ukraine Conference' (Just Security, 2 March 2023) <https://www.justsecurity.org/85336/can-aid-or-assistance-be-a-use-of-force-expert-qa-from-stockton-centers-russia-ukraine-conference/>, accessed 1 May 2024.

War of the Future: Drones Playing a Significant Role in the Ukraine War (i24news, 2023) <https://www.i24news.tv/en/news/ukraine-conflict/1677160351-war-of-the-future-drones-playing-a-significant-role-in-the-ukraine-war>, accessed 1 May 2024.

NON-PLAGIARISM DECLARATION

Utrecht University considers any form of academic dishonesty to be a very serious offense. Utrecht University expects each student to be familiar with and to observe the norms and values that ensure academic integrity. The most serious forms of deception that can impair this integrity are fraud and plagiarism.

These types of conduct are prohibited, not only because they undermine a fair assessment of students' work but also because they cause unfairness to peer students. Plagiarism and fraud deny your opportunity to learn and show disrespect for scholars to whom the work should be credited.

Plagiarism is a form of fraud and is defined as the wrongful appropriation of another author's work without proper citation. Utrecht University's website on "Fraud and Plagiarism" elaborates on what may be considered fraud or plagiarism: https://students.uu.nl/en/practical-information/policies-and-procedures/fraud-and-plagiarism.

1. I declare that the master's thesis entitled A Comprehensive Analysis of Privacy and Data Protection in Conflict Affected Areas: Revising human rights and humanitarian law to Address the challenges of Surveillance Technologies which is submitted for the award of LLM in Public International Law is my own work and does not involve fraud or plagiarism.

2. I also declare that the aforementioned master's thesis has not been submitted by me in any other universities for the degree of diploma.

Signature[1]: M. Rahimi

Name: Masoumeh Rahimi

Date: 28 June 2024

[1] You can digitally sign the form. Or you can print out this form, sign it, and send a scanned copy of the form.