International Review of the Red Cross (2023), **105** (923), 1152–1162.
Organized crime
doi:10.1017/S1816383123000103

IRRC

BEYOND THE LITERATURE

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

Edited by Russell Buchan and Asaf Lubin*

In this new series called "Beyond the Literature", the Editorial Team of the *International Review of the Red Cross* selects a recently published volume in the field of humanitarian law, policy and action and convenes a discussion on the book among experts, in an effort to foster constructive engagement on some of the most promising recent literature in the field.

Every so often, a book comes along that engages in a uniquely thoughtful and in-depth way on an issue of pivotal contemporary importance. Russell Buchan and Asaf Lubin's recently published edited volume, The Rights to Privacy and Data Protection in Times of Armed Conflict, *is one such book.*

The book, published in June 2022, aims to address the unique threats posed by contemporary armed conflict to the rights to privacy and data protection. The editors and the chapter authors they have convened address the many – and ever-changing – technological advances in surveillance, data analytics, artificial intelligence and more, and how these advances fundamentally alter the landscape and nature of military operations in the modern world. Even more to the point, the book delves into the gaps in existing law and policy that, as they stand,

* Published by NATO CCDCOE, 2022.

fail to adequately address the implications of these advances for privacy and data protection rights.

In this inaugural voyage for the Review*'s "Beyond the Literature" series, we have invited Russell and Asaf to introduce their volume, before then posing a series of questions to Jelena Pejic, Marko Milanovic and Eduardo Ustaran, who have graciously agreed to act as discussants of the book, given their expertise in the international humanitarian law (IHL), international human rights law (IHRL) and data protection fields. Jelena worked for many years as Senior Legal Adviser to the International Committee of the Red Cross (ICRC) and has published widely on IHL. Marko is Professor of International Law at the University of Reading and is co-editor of the Tallinn Manual 3.0 project, which examines the application of international law to cyber operations. Marko is an expert in IHRL and has published extensively in that field. Eduardo is a data protection expert and, being a partner at Hogan Lovells International LLP, he brings an important practitioner's perspective to the debate.*

: : : : : : :

Bruno Demeyere: ***Russell and Asaf, what motivated you to write this book? What message does the book convey?***

Russell Buchan and Asaf Lubin: In *A Memory of Solferino*, the Swiss humanitarian Henry Dunant laid the foundations for the worldwide Red Cross and Red Crescent movement. The book ends with a series of questions that Dunant leaves for his readers. These questions have survived the test of time. One of them reads: "[I]n an age when we hear so much of progress and civilization, is it not a matter of urgency, since unhappily we cannot always avoid wars, to press forward in a human and truly civilized spirit the attempt to prevent, or at least alleviate, the horrors of war?"[1]

The charge that Dunant led remains as relevant today as it was at the end of the Battle of Solferino of 1859. While the theatre of war and its instrumentalities have morphed and evolved, superfluous injury and unnecessary suffering are still commonplace. These wartime harms now manifest in both physical and digital form. Cyberspace is now a new frontier for violence wherein data is considered a strategic military asset and technologies of surveillance, censorship, hyper-connectivity, automation and disinformation are the state of the art. Against this backdrop there is again urgency in rethinking the regulatory tools at our disposal to constrain this contemporary arms race and hold accountable national armed forces, paramilitary groups and their contractors when abuses of power ultimately take place.

The main bodies of IHL – the Hague Conventions of 1899 and 1907, the Geneva Conventions of 1949, and the Additional Protocols of 1977 – were all

1 Henry Dunant, *A Memory of Solferino*, 1862 (reprinted in English by the ICRC, 2010), p. 127.

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

produced in a pre-internet age. These treatises thus lack any reference to the function that informational privacy, online freedom of expression, data protection and cyber security could play as important shields to protect civilians from the effects of modern wars. This legal vacuum has not stopped militaries and the tech giants that support them from developing and deploying big-data collection and analysis tools, machine learning algorithms, facial recognition software, and surveillance drones and satellites, to name a few examples. *The Rights to Privacy and Data Protection in Times of Armed Conflict* offers an assessment of existing and future IHL and the concurrent application of IHRL as legal frameworks that could respond to these developments.

The book was commissioned and published by the NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. We were invited to act as its general editors and we benefited immeasurably from the support and guidance of Ann Väljataga, a legal researcher at the CCDCOE. The focus of the book is on the protection of the rights to privacy and data protection in times of armed conflict, which is an important yet under-researched topic in the literature. The book brings together a talented group of scholars drawn from a range of different backgrounds, and we believe it will be of broad appeal to researchers, practitioners, policy-makers and other stakeholders working across the disciplines of technology, human rights, international law and international relations.

As we write in the book's introduction: "In light of the technological advances in the fields of electronic surveillance, social engineering, predictive algorithms, big data analytics, artificial intelligence, automated processing, biometric analysis, and targeted hacking, we presented our contributing authors with a Herculean task. We asked each author to doctrinally and theoretically explore the ways that these technologies, and others, are already interacting or could possibly interact in the future with wartime digital rights. In so doing, we invited the authors to grapple with the concurrent and extraterritorial application of these rights, with the limitations and possible derogations from these rights during war, and with their scope of application to actual case studies and scenarios taken from the field."[2]

The book is split into four parts which cut across different themes. Part 1 explores the extent to which various regimes of IHL protect the rights to digital privacy and data protection. In Chapter 1, Mary Ellen O'Connell advances the argument that the protection afforded by international law to personal data is the same during times of armed conflict as it is during times of peace. In Chapter 2, Tal Mimran and Yuval Shany zero in on the weapons review obligation contained in Article 36 of Additional Protocol I [AP I], arguing that it requires State parties to integrate privacy concerns into their evaluation of new military technologies. In Chapter 3, Laurie Blank and Eric Talbot Jensen examine the extent to which international humanitarian law governs the seizure, destruction and requisition of data during times of armed conflict. In Chapter 4, Jacqueline Van De Velde assesses the extent to which the law of neutrality requires neutral

2 *The Rights to Privacy and Data Protection in Times of Armed Conflict*, p. 4.

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

States to monitor and prevent companies located within their jurisdictions from transferring data to parties to armed conflicts in breach of the rights to privacy and data protection. In Chapter 5, Omar Shehabi explores how the law of occupation, and in particular the obligations it imposes upon Occupying Powers, can be progressively reinterpreted to protect digital privacy. In Chapter 6, Emily Crawford examines the privacy-related rights of prisoners of war [PoWs] in the digital age and, in particular, identifies the types of data that Detaining Powers can collect from PoWs.

Part 2 of the book considers the impact of surveillance technologies on the enjoyment of digital rights. In Chapter 7, Leah West explores the legal obligations arising during armed conflict that limit the use of facial recognition technology by belligerent parties. In Chapter 8, Eliza Watt examines the impact of sustained drone surveillance on non-combatants in war zones and analyzes the legal constraints placed by IHL and IHRL on this practice. In Chapter 9, Tara Davenport analyzes the international legal rules that apply when parties to armed conflicts collect data stored on or passing through underwater sea cables.

Part 3 of the book examines the obligations of militaries and humanitarian organizations when it comes to the protection of digital rights. In Chapter 10, Tim Cochrane explores the potential of individuals to obtain personal data from military agencies under the legal regimes of several States, namely Australia, Canada, New Zealand and the United Kingdom. In Chapter 11, Deborah Housen-Couriel focuses on data sharing within multilateral military operations. In Chapter 12, Asaf Lubin examines the obligations of international organizations to protect data in the context of their humanitarian action; this chapter uses the ICRC as a case study and may be of particular interest to the participants today.

Part 4 analyzes the protection of digital rights in the *jus post bellum*. In Chapter 13, Kristina Hellwig examines the role of the right to privacy in the investigation and prosecution of international crimes. In Chapter 14, Yaël Ronen considers the "right to be forgotten" – that is, the right of individuals to have digitalized personal information removed from the public sphere. Finally, in Chapter 15 Amir Cahane proposes a "right not to be forgotten", which, in order to protect digital identities, would place a moratorium on private tech companies and prevent them from denying individuals caught up in humanitarian crises access to their online accounts.

The book was launched at CyCon, a cyber security conference convened by NATO's CCDCOE, in early June 2022. Jelena, Marko, and Eduardo first discussed the book at CyCon, and we thank all three for their thoughtful engagement with the book, both at CyCon and here.

Bruno Demeyere: ***Marko, Eduardo and Jelena, do you share the book's primary premise that digital rights, such as privacy and data protection, are more vulnerable to abuse in times of armed conflict and that there is a need to examine the practice of militaries and the law that constrains them in this area?***

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

Jelena Pejic: To be honest, my sense is that we are losing – or have already lost – the battle for privacy and data protection in all spheres of life, whether in peacetime or armed conflict. The fast-paced development of technology and the opaqueness of governments and other relevant actors about their capabilities simply outstrips our ability as individuals to know what information about us is being collected, stored, and shared – i.e., processed. Having said that, persons affected by armed conflict, civilians and detainees in particular, are inherently vulnerable to abuse and have even less control over the exploitation of data related to their real or digital lives in the disrupted circumstances of war. In addition, the problem of protecting digital rights in armed conflict is likely to become more significant over time. *Sauf erreur* on my part, militaries have not engaged with this consequence of their operations in a meaningful way. I thus agree with the statement in the question above.

Marko Milanovic: I do. If only a few years ago somebody wrote a book (or a book chapter) about privacy in armed conflict, most international lawyers would have thought the author(s) to be slightly mad. Privacy is not something we normally associate with war. Soldiers in trenches seem as far removed from privacy as anything can be. And even the literature on human rights in armed conflict and the relationship between IHRL and IHL has focused on more "tangible" or physical rights, such as the right to life or liberty of person. A great success of this book is how all of its chapters expose such views as misplaced. Privacy in armed conflict is not science fiction. Take any modern conflict – including the ongoing war in Ukraine – and just consider how the advent of the digital age has made severe impacts on the right to privacy inevitable, and how such impacts need to be regulated. From cyber attacks affecting civilians, for example involving the exfiltration or destruction of their data, to surveillance measures implemented by occupying authorities against the civilian population, to the collection of biometrics and other data of PoWs – all of these are examples of privacy being adversely affected in armed conflict, with or without justification. In all of these cases harm is being inflicted not just on a party to a conflict, whether a State or an armed group, but on numerous individuals *qua* individuals. It is only right and proper for human rights law to take such harms into account. States that care about their reputation as law-abiding members of the international community need to take their obligations in this regard seriously. And their officials need to read this book!

Eduardo Ustaran: Absolutely. The ongoing war in Ukraine has certainly shown the crucial importance of privacy and data protection in times of armed conflict. For example, the privacy implications presented by activities such as the use of facial recognition technology to help identify the bodies of soldiers killed in combat and track down their families in order to inform them of their deaths are substantial. Equally, the procurement by the military of location data surreptitiously obtained from mobile devices and apps raises similar issues. These are use cases that under other circumstances would certainly require undertaking

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

a "data protection impact assessment", and the fact that they are occurring during a war does not take away that need.

Disinformation and cyber attacks are an essential part of modern warfare and are directly affected by key data protection principles like data accuracy and integrity. Cyber security in particular is a key defensive pillar well beyond the theatre of war. The need to adopt cyber security best practices – from strengthening firewall protection and keeping software and backups updated to (re-)training employees and reviewing incident response plans and contractual arrangements – has never been more real. So, if there is an area of data protection law that is likely to be tested during a war, data security will be a top candidate.

All of this shows that the role of privacy and data protection rights does not stop when the shelling starts. If anything, it becomes more life-critical, but as with anything affected by war, it needs to adapt to its specific reality. Data protection impact assessments may need to be more agile, data security more robust and data sharing more focused, but ultimately, wars do not change our dignity or our fundamental rights. Data protection on the battlefield may look different, but it is very much a pressing need.

Bruno Demeyere: ***Which of the book's chapters or themes did you find most illuminating, and why?***

Jelena Pejic: All the book's chapters address different angles of the topic and are worth reading, so it would be unfair to single out one in particular. Personally, I was most absorbed by the contributions dealing with the effects of certain surveillance technologies and weapons/platforms on respect for privacy and data protection. As explained in the book, there is a tension in armed conflict between the legal and operational requirements of the parties to an armed conflict to gather information and intelligence – in order to, for example, properly identify military objectives and apply other IHL targeting rules – and the privacy rights of the affected local population and individuals. Ensuring respect for digital rights to a greater degree than is currently the case would appear to be possible provided there is an awareness of the potentially nefarious consequences of indiscriminate information gathering over time and, of course, a will to do so. My sense, however, is that there is a significant practical difference in this regard between measures that could be taken in the conduct of hostilities and those that could be taken in relation to persons detained by a party to a conflict. The book could not make this sufficiently clear, due to the fact that it is an edited volume of separate chapters and not a monograph – but the practical distinctions would be worth exploring going forward.

Marko Milanovic: The chapters in the book are uniformly excellent, accessible and readable, and that is a very rare thing in an edited collection. But I was particularly struck by some of the chapters, which I thought were especially novel and thought-provoking – for example, the chapter by Mimran and Shany, whose thesis is that the

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

human right to privacy needs to be integrated into weapons reviews pursuant to Article 36 of AP I. Or there is the illuminating chapter by Shehabi on digital privacy in the occupied Palestinian territories and the multitude of ways in which Israel as the Occupying Power subjects the Palestinian population to systemic and pervasive surveillance. The chapter by Crawford on PoWs is incredibly relevant – again, just consider the collection, processing and dissemination of data about PoWs in the ongoing conflict in Ukraine. The chapter by West on facial recognition and its role in applying the principles of precaution and distinction in the targeting process is very cautionary. Finally, there is the chapter by Hellwig on the *jus post bellum* and the numerous privacy and data protection issues that arise in the context of gathering evidence for international criminal prosecutions.

Eduardo Ustaran: As a data protection lawyer, for me those chapters that analyze the question of whether existing legal frameworks are suited to address the specific data uses that take place in an armed conflict scenario are particularly thought-provoking. The opening chapter masterfully deals with the existing protections for personal data, looking at the role of IHL and IHRL. These protections, of course, also apply to personal data during armed conflicts. It is also very interesting to see the debate that emerges between the school of thought which argues that laws such as the General Data Protection Regulation [GDPR] are precluded from applying to data activities in situations of armed conflict, and the idea that national security exemptions are in fact limited and do not necessarily prevent the full application of data protection law.

Taking this multi-pronged approach to the protection of privacy and personal data even further, several other chapters are also able to introduce creative ways of thinking about how the combination of legal approaches can be effective in this context. From the applicability of Article 36 of AP I – which requires determining whether the employment of a new weapon would be prohibited under international law – to the potential applicability of the "right to be forgotten" as a mechanism of privacy preservation in cyberspace, there is no shortage of points of view that bring together legal authorities to show a kaleidoscopic approach to the issues at stake.

But while the legal theories put forward by the various authors provide a truly illuminating perspective, they are greatly balanced by the many practical overviews of real-life scenarios, including in particular the challenges raised on the ground by the emergence of sophisticated surveillance technologies. These are technologies that are currently being applied across many different parts of the world and that affect non-combatants in armed conflicts, and they highlight the need for the application of minimum safeguards.

Bruno Demeyere: ***The book highlights two legal approaches for the future regulation of privacy and data protection in war: one that extends the existing rules of IHL to cover new types of data-intrusive activities by both militaries and non-State groups involved in armed conflict, and another that relies on the***

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

concurrent application of human rights law to achieve similar effects. Which of these two approaches do you find more persuasive? Should they be tied together or should a third approach be considered for thinking about regulation in this space?

Jelena Pejic: This is a tough one, and I am afraid there is no satisfactory answer. It is a fact that IHL contains only a few articles pertaining, mainly by implication, to the right to privacy and data protection, and several more that could be interpreted as relevant to it. (In this context I was struck by Eliza Watt's chapter in the book, in which she argues that the duty of constant care in military operations could serve to fill the normative gap in the IHL framework by placing privacy and data protection obligations on States' intelligence operations. Needless to say, it would be useful to know what States may think.) Given that the Geneva Conventions and AP I were developed well before the ongoing technological revolution, this is not surprising. A separate legal challenge would be how to deal with the privacy or data protection "obligations" of non-State armed groups given the dearth of binding IHL rules in non-international armed conflict and the fact that non-State armed groups are not the addressees of human rights law.

As regards human rights law, many legal issues arise, of which two of a basic nature come to mind. First, what exactly is the difference between privacy and data protection, and are both equally relevant in armed conflict? I have not been able to find a satisfying, comprehensive description of the difference for the purposes of a possible response. Second, what exactly is meant by human rights "law"? Is it binding law of global import, of which there is little, or regional hard law, whose geographic reach is obviously limited? It should be noted that even the European Union's 2016 General Data Protection Regulation, looked to by non-EU actors as a model in this domain, excludes from its ambit data protection linked to national security.[3] Or is human rights "soft law" meant? While there is plenty of it, these norms are non-binding and are very rarely tailored to the specificity of armed conflict, due to which their application would likely remain aspirational.

Thus, a third way could be explored, one which would carefully examine the relevant IHL norms and even more carefully parse out the relevant norms of human rights law on privacy and data protection that would be feasible in armed conflict. Such an effort was, for example, undertaken in the humanitarian sector, resulting in the *Handbook on Data Protection in Humanitarian Action* published by the Brussels Privacy Hub and the ICRC.[4] The ICRC and other

3 Regulation (EU) No. 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 OJ (L 119), 2016 (GDPR). According to Article 2, as elaborated in the preamble of the Regulation, the GDPR does not apply to "issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. The Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union." Preamble, para. 16.

4 Brussels Privacy Hub and ICRC, *Handbook on Data Protection in Humanitarian Action*, 2nd ed., 2020.

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

organizations working in this field have also developed their own documents and guidance on the matter.

Marko Milanovic: I don't think it's an either-or kind of choice. A legal system can adapt to new developments through a combination of new law and the evolution of old law, and in our case the recognition that some parts of the old law which were thought to be irrelevant are actually quite relevant. There is no barrier to applying existing rules of IHL and IHRL to novel questions of the digital age, including the right to privacy of civilians and combatants. What I would say in this context, however, is that IHRL is inevitably going to be more important in this evolutionary process than IHL, for two basic reasons. First, politically it seems highly unlikely that States will agree to new bespoke rules of IHL that address privacy issues in armed conflict. Second, current IHL, even in the abstract, says little or nothing on these issues. There is very little material here that can evolve. This is nothing like questions of deprivation of life and liberty during armed conflict, where IHL has detailed rules on the matter that can in some sense take priority over more general rules of IHRL by applying some variant of the *lex specialis* principle. That really can't be done with privacy or many other human rights, from freedom of expression to most socio-economic rights, on which IHL is simply silent. So, the only option really is to apply human rights law in a more flexible, realistic manner so as to take into account the extraordinary circumstances of armed conflict.

Bruno Demeyere: ***Given the oversized role that private-sector companies play in the development and deployment of the relevant infrastructures and applications under examination in this book, is there room to reconsider the role of non-State actors in the development of relevant rules of IHL and IHRL in this space? What categories of rule developers should play a role in the prescriptive process that could lead to the future regulation of wartime digital rights?***

Jelena Pejic: I am not sure one should immediately embark on a prescriptive process, as there are many issues related to the law, technology, and military policy and practice – and their interface – that should first be identified and discussed. Given that armed conflict is the context, such an exchange should involve all relevant actors: this would mean governmental and relevant intergovernmental representatives, as well as military lawyers and practitioners, private-sector/tech company experts, the ICRC and other relevant humanitarian organizations, non-governmental organizations working in the field, and academics dealing with the matter. Each could bring their perspective to the table, allowing for an overview of what may be feasible given the novelty of the issue. To give an example, the requirement of consent is a cornerstone of human rights-compliant data protection regimes in peacetime. In those circumstances, consent as a legal basis for processing personal data "must be freely given,

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

informed, specific, and an unambiguous indication of wishes by a clear affirmative act signifying agreement to processing".[5] Can this principle be applied to information gathering, data processing etc. in armed conflict? If so, how? In the conduct of hostilities? To detained persons? Would adaptations in its implementation need to be made? How?

Bruno: ***Are there any issues – legal, technological, political, social or economic – that the book fails to capture? What should future research in this area focus on?***

Jelena Pejic: My sense is that drilling down into some of the thorny issues would be more useful than pursuing a broad, academic approach to the subject matter. Some chapters of the book would lend themselves to such an in-depth "rubber meets the road" examination. Another option would be to try and identify those privacy and data protection principles and rules that could – and should – be applicable in armed conflict, such as lawfulness, purpose limitation, minimization, storage limitation, data security and accountability, to name a few. Whatever path may be chosen, there is much work ahead.

Marko Milanovic: The book does its task admirably, but there will always be questions open for further research: first, the regulation of intelligence gathering – including intelligence sharing – from the standpoint of IHRL but during armed conflict; second, the issue of privacy of PoWs that the book already examines, which will inevitably get litigated in the near-to-medium term; third, cyber attacks that destroy or exfiltrate private data or otherwise impact private life, for example the leaking of the health-related information of enemy officials online. Note how in terms of IHL this issue has so far been analyzed from the perspective of whether data can constitute a (civilian) object, but from an IHRL perspective this is irrelevant – even if data is not an object, and destroying it does not constitute an attack within the meaning of IHL, destroying it could nonetheless violate the human right to privacy. Finally, there is the issue of extraterritorial application of IHRL in situations of armed conflict to violations of privacy, where again the Ukraine conflict is an instructive case study.

Eduardo Ustaran: The book demonstrates that the data activities which take place during armed conflict require a multi-pronged approach to regulation that combines various existing frameworks and regulatory approaches. In my view, the complexities of such data activities are best addressed through the interlinked combination of IHL, human rights law and existing data protection law. Flowing from the issues discussed above, perhaps the area that may merit a more in-depth analysis in future books is the role of data protection law in regulating the use of personal information in armed conflict. Data protection law, understood as the

5 European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law*, 2018 ed., pp. 101, 111.

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press

body of law tasked with regulating the use and protection of personal information, is likely to play an increasingly relevant role in this particular context.

In this regard, it would be extremely interesting to explore how the principles, rights and accountability obligations that are present in the GDPR and similar frameworks can and should be adapted to deal with the use of data in times of armed conflict. Specific and well-established principles such as fairness, purpose limitation and data minimization are likely to play a truly vital role in this environment. The scope of data protection rights – in particular, newer rights such as the right to object to automated decision-making – should be explored, as well as the most appropriate governance processes that State and private-sector actors would need to deploy to ensure observance of universal principles. There is much that can be learnt from the responsible use of data in peacetime and that could be successfully deployed during armed conflicts. Ultimately, through the combination of legal approaches and the deployment of tried and tested data protection practices, it may be possible to limit some of the horrors of war in the data realm.

https://doi.org/10.1017/S1816383123000103 Published online by Cambridge University Press