CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Reflections on the Afterlife: Which Rules Govern the Post-Occupation Retention and Use of Personal Data Collected by the Military?

Tatjana Grote
PhD Candidate
School of Law
University of Essex
Colchester, United Kingdom
t.grote@essex.ac.uk

Abstract: The collection of personal data by the military has become a commonplace practice in situations of military occupation. However, there has been barely any scholarly engagement with the post-occupation afterlife of such data. This paper explores the question of which legal regime governs the retention and use of personal data collected during a military occupation once the former occupying power is no longer in a position to exercise territorial control. It argues that as long as physical control over territory or a person is required to establish the extraterritorial applicability of international human rights law (IHRL), the pertinent IHRL treaty provisions will no longer be applicable to personal data collected during an occupation once a former occupying power ceases to exercise territorial control. While the law of occupation is traditionally equally premised on physical control, there is a convincing case for the continuous applicability of certain international humanitarian law (IHL) provisions based on a functional approach to the law of occupation. Although the relevant IHL norms do not protect privacy as an end in itself and hence offer only very limited protection, they might constitute the only available legal safeguard regarding the post-occupation retention and use of personal data if and to the extent that data protection law and IHRL are inapplicable.

Keywords: *personal data, international humanitarian law, international human rights law, military occupation, post-occupation law*

1. INTRODUCTION

When the United States Armed Forces left Afghanistan, they left behind, *inter alia*, handheld interagency identity detection equipment (HIIDE),[1] which is used to collect biometric data, identify individuals and access contextual information on them.[2] Part of this data has now most likely become accessible to the Taliban, putting many Afghans at a considerable risk of retribution.[3] This example is emblematic of two relatively recent developments: First, personal data collection has become an integral part of military control.[4] Second, the afterlife of such data can be highly relevant to the well-being of civilians.

So far, the academic debate on data protection and armed conflict has focused either on the rules relating to the conduct of hostilities[5] or the collection of data during a belligerent occupation.[6] Issues related to the post-conflict or post-occupation storage and use of personal data collected by the military, on the other hand, have received barely any attention.

This lack of scrutiny is concerning as personal data is a highly sought-after resource that equips a belligerent party with a temporally unlimited form of influence. Even long after the end of an occupation, the data collected by a belligerent party could become a threat to the data subject when falling into the hands of malign actors. Equally, the belligerent party itself might continue using the data it collected to exercise remote control over the behaviour of data subjects, such as by threatening to publish harmful information.

1 Leah West, 'Face Value: Precaution versus Privacy in Armed Conflict' in Asaf Lubin and Russell Buchan (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE Publications 2022) 132–133.

2 ibid 133.

3 Human Rights Watch, 'New Evidence That Biometric Data Systems Imperil Afghans' (30 March 2022) <https://www.hrw.org/news/2022/03/30/new-evidence-biometric-data-systems-imperil-afghans> accessed 27 November 2023.

4 Asaf Lubin, 'The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law' in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law* (Edward Elgar Publishing 2022) 465; Marten Zwanenburg, 'Know Thy Enemy: The Use of Biometrics in Military Operations and International Humanitarian Law' (2021) 97 International Law Studies 1405, 1411–1413.

5 See eg West (n 1); Tim McCormack, 'International Humanitarian Law and the Targeting of Data' (2018) 94 International Law Studies 222; Kubo Mačák, 'Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law' (2015) 48 Israel Law Review 55; Heather A Harrison Dinniss, 'The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives' (2015) 48 Israel Law Review 39.

6 Rohan Talbot, 'Automating Occupation: International Humanitarian and Human Rights Law Implications of the Deployment of Facial Recognition Technologies in the Occupied Palestinian Territory' (2020) 102 International Review of the Red Cross 823; Omar Yousef Shehabi, 'Emerging Technologies, 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 Conflic*t (NATO CCDCOE Publications 2022).

This paper provides a preliminary analysis of one of the most crucial legal questions raised by this phenomenon: which law governs the post-occupation retention and use of civilian personal data[7] collected by the military?

This particular focus reflects the gap in the literature highlighted above as well as the practicalities of data collection: Collecting personal data will often only be possible and conducive to the security needs of a belligerent party once the armed forces repeatedly encounter civilians outside of a situation of hostilities, such as when exercising somewhat permanent control.[8] Moreover, the following discussions will centre around the law governing international armed conflict (IAC). While data collection might also be increasingly relevant in non-international armed conflict (NIAC),[9] the risk of a significant gap in protection is far smaller since post-conflict state conduct would be governed by IHRL.

Note that, in principle, domestic data protection law could apply to the phenomenon this paper is concerned with. However, if such laws exist,[10] activities relevant to national security will frequently be excluded from the scope of peacetime data protection legislation.[11] Moreover, domestic data protection law might not apply to foreign armed forces. Hence, without prejudice to the particularities of a specific body of domestic law, IHL and IHRL will most likely be the two main legal frameworks of relevance to military data collection and use when connected to an international armed conflict.

This paper argues that there is a convincing case for the continuous applicability of certain IHL provisions. While the protection provided by IHL will most likely be very minimal, since IHRL will no longer be applicable once a belligerent party ceases to exercise physical control over a person or territory, it might constitute the only available legal safeguard regarding the long-term storage and use of personal data collected in situations of military occupation.

7 The term personal data is understood as in art 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation) [2016] OJ L119.

8 Zwanenburg (n 4) 1408.

9 Myanmar is one example of this tendency; International Crisis Group, 'Myanmar's Military Struggles to Control the Virtual Battlefield' (18 May 2021) <https://www.crisisgroup.org/asia/south-east-asia/myanmar/314-myanmars-military-struggles-control-virtual-battlefield> accessed 28 October 2023.

10 Note that Afghanistan, for instance, did not have a data protection law at the time; Human Rights Watch (n 3).

11 See GDPR art 2(2)(a), (b) and (d). Some have also questioned the applicability of data protection law during armed conflict in general; see Robin Geiss and Henning Lahmann, 'Protection of Data in Armed Conflict' (2021) 97 International Law Studies 556, 568.

2. DOES IHRL APPLY TO THE POST-OCCUPATION RETENTION AND USE OF MILITARY PERSONAL DATA?

Regarding issues arising in the aftermath of conflict, IHRL might be a more appropriate point of departure than IHL. In NIAC, state parties act within their own territory, where IHRL would certainly be applicable *ratione loci*. In IAC, on the other hand, IHRL can only be relevant if and to the extent that it binds states when they are acting extraterritorially.[12] Consequently, there is a need to assess whether IHRL applies to the long-term storage and use of data collected during military occupation.

A. How Does the Post-Occupation Retention of Personal Data Relate to the Accepted Models of the Extraterritorial Applicability of IHRL?

It is by now fairly accepted that IHRL will apply extraterritorially when a state exercises effective control over foreign territory or when a state agent 'exercises control and authority over an individual'.[13] Note that the effective control over territory standard is considered to require a lower level of control than Article 42 Hague Regulations (HR).[14] Hence, most would agree that as long as and where territory is occupied within the meaning of Article 42 HR, IHRL will be applicable *ratione loci*.[15] What happens, however, once a belligerent occupation ends?

The underlying issue in this respect is the following: data-facilitated control can impact an individual's enjoyment of human rights outside of the acting state's territory without that state exercising any kind of physical control over that individual. So far, both above-mentioned tests have been applied exclusively in situations where the control or authority in question was physical. While the effective control-test quite clearly refers to territory, the state agent authority-test could be interpreted to encompass purely virtual control over an individual. However, there is no jurisprudence confirming such an interpretation in the context of digital privacy. Consequently, it seems fair to assume that the established theories of extraterritorial applicability of IHRL currently do not encompass situations in which control is purely virtual.

12 Note that this would not necessarily be the case if the relevant rights – in this case, the right to (digital) privacy – were part of customary international law. However, given the lack of uniformity when it comes to the precise content and protection of a right to digital privacy, this author agrees with others who do not consider this to be the case. See Eliza Watt, *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law* (Edward Elgar Publishing 2021) 141.

13 *Al-Skeini and Others v United Kingdom* [2011] ECtHR [GC] 55721/07 [74]. See also UN Human Rights Committee, 'General Comment No. 31' (29 March 2004) UN Doc CCPR_C_21_Rev.1_Add.13-EN para 10.

14 Hanne Cuyckens, *Revisiting the Law of Occupation* (Brill Nijhoff 2017) 174; Tom Ruys and Sten Verhoeven, 'DRC v. Uganda: The Applicability of International Humanitarian Law and Human Rights Law in Occupied Territories' in Roberta Arnold and Noëlle Quénivet (eds), *International Humanitarian Law and Human Rights Law: Towards a New Merger in International Law* (Brill Nijhoff 2008) 179.

15 Noam Lubell, 'Human Rights Obligations in Military Occupation' (2012) 94 International Review of the Red Cross 317, 319.

B. Alternative Approaches to Establishing the Applicability of IHRL to Personal Data

The United Nations Office of the High Commissioner for Human Rights (OHCHR) has suggested that the applicability of IHRL can be determined by answering the question of which state physically controls the location of the server or device on which the data is stored.[16] This approach is unconvincing, however, since states could simply eschew their IHRL obligations by storing data on a server or device they do not have physical control over.[17] Moreover, from a practical perspective, it might be nearly impossible to identify the physical location of the data in question, especially if such data has been copied to multiple servers or devices.

Others have suggested moving away from control-based models altogether and endorsed, instead, a cause-effect approach to the extraterritorial applicability of IHRL. Whereby, whenever state behaviour has a negative effect on the enjoyment of human rights abroad, the negative human rights obligations of the respective state regarding the affected right or rights would be applicable.[18] The idea underlying this approach has gained prominent scholarly support[19] and has surfaced in General Comment No. 36.[20] While the details of such an interpretation would need to be worked out, this author considers it a suitable response to technological and environmental developments that can enable a substantial impact on the enjoyment of certain rights abroad without physical control over the affected individuals. However, the approach has not (yet) been endorsed by any international court in the context of the right to privacy.

In sum, physical control over territory or over a person remains a necessary requirement for the extraterritorial applicability of most human rights treaties. Consequently, under current international law, the long-term storage and use of data collected during a military occupation will, if at all, be governed by IHL.

16 UN Office of the High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37 para 34.

17 See also Marko Milanovic, 'Surveillance and Cyber Operations' in Mark Gibney (ed), *The Routledge Handbook on Extraterritorial Human Rights Obligations* (Routledge 2021) 374–375.

18 ibid 373–375; Marko Milanovic and Michael N Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations during a Pandemic COVID-19' (2020) 11 Journal of National Security Law and Policy 247, 263; Marko Milanovic, *Extraterritorial Application of Human Rights Treaties* (Oxford University Press 2011) 209–219.

19 Yuval Shany, 'Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law Borders and Human Rights' (2013) 7 Law & Ethics of Human Rights 47, 67–71. While Shany agrees with the general idea of moving away from control-based standards, he proposes a different, functional approach that emphasizes the intensity of the power and special legal relations between a state and an individual as factors to be taken into account when determining the existence and extent of extraterritorial human rights obligations.

20 UN Human Rights Committee, 'General Comment No. 36' (3 September 2019) UN Doc CCPR/C/GC/36 para 63.

3. DOES IHL APPLY TO THE POST-OCCUPATION RETENTION OF MILITARY PERSONAL DATA?

Generally, IHL applies once an armed conflict erupts or an occupation is established. It should be noted that certain rules come with specific applicability regimes. Hence, there is a need to evaluate which parts of IHL would apply to the post-occupation storage and use of military data.

A. Which Parts of IHL Are of Relevance, and Which Provisions Govern Their Applicability?

As explained above, military data has, so far, mostly been discussed from a conduct of hostilities perspective. Mass collection of civilian personal data, however, is most common in situations where the military exercises stable control.[21] The rules applicable to such situations would, thus, seem a natural starting point from which to address the question at hand.

Traditionally, the applicability of the law of occupation has been considered to be defined by Article 42 HR: 'Territory is considered occupied when it is actually placed under the authority of the hostile army'.

There has been some debate amongst scholars on whether the adoption of Geneva Convention IV (GCIV), by virtue of its Article 4(1), broadened the scope of the law of occupation to all situations in which a protected person finds themselves 'in the hands of' a belligerent party. However, the most recent International Committee of the Red Cross (ICRC) commentary on Geneva Convention III (GCIII) clarifies that it is Article 42 HR that defines the concept of occupation and that 'subsequent treaties, including the Geneva Conventions, have not altered this definition'.[22] Yet, the 'in the hands' standard still defines the personal scope of the general protections of GCIV. Both standards, therefore, are of relevance to this paper.

This paper argues that both Article 4(1) GCIV and Article 42 HR traditionally refer to the same type of control, namely physical control over territory or persons. In the case of Article 42 HR, this is evident from the wording of the provision, which links the concept of occupation with territory. Many would agree that the effective control required by Article 42 HR can only be established through the actual or

21 The most prominent examples of military data collection during armed conflict are the operations carried out by the United States in Afghanistan, Iraq and Israel in the occupied Palestinian territories.

22 ICRC, *Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War* (Cambridge University Press 2021) para 327.

potential presence of 'boots on the ground'.[23] Even those arguing that remote control can be sufficient to establish a belligerent occupation consider that it is the potential of *physical* control, as opposed to merely virtual control, that justifies such an interpretation.[24] This can be understood as a corollary of the idea that the authority required by Article 42 HR needs to be exclusive.[25] Even nowadays, it is difficult to imagine a situation where purely virtual influence would be sufficient to establish exclusive control.

The commentary to GCIV suggests that 'in the hands of' is similarly defined with reference to physical control. While the concept might be broader than that of occupation, the ICRC commentary nevertheless defines it with reference to control over territory.[26] When the commentary states that the concept 'need not necessarily be understood in the physical sense',[27] this clarifies that a person does not need to be under the direct, physical control of a belligerent party. However, at least traditionally, an individual would still need to be located in territory that is or can be brought under the physical control of a belligerent party to qualify as a protected person. Hence, it seems that it is rather the stability and potentially the level of control that distinguishes a situation in which a person is in the hands of a belligerent party from a situation of occupation – not the type of control.

B. How Does Data-Facilitated Control Challenge the Current Legal Framework?

As Lieblich and Benvenisti note, 'While the law of occupation assumed, traditionally, physical control on the ground, control can nowadays be exercised through various measures.'[28] Retaining sensitive personal data will allow a belligerent party to take precisely such measures of control that are not premised on ongoing physical dominance.[29] For instance, a belligerent party could threaten to publish or share certain sensitive data to coerce a data subject into a specific course of action. It could further use the collected data to pretend to be the data subject to the personal and/or economic detriment of the latter.

23 Orna Ben-Naftali, 'Belligerent Occupation: A Plea for the Establishment of an International Supervisory Mechanism' in Antonio Cassese (ed), *Realizing Utopia: The Future of International Law* (Oxford University Press 2012) 541; Yoram Dinstein, *The International Law of Belligerent Occupation* (Cambridge University Press 2009) 50. The presence of foreign troops has been considered a necessary component for the establishment of a belligerent occupation by the ECtHR in *Sargsyan v Azerbaijan* and *Chiragov v Armenia*; *Sargsyan v Azerbaijan* [2015] ECtHR [GC] 40167/06 [94]; *Chiragov and Others v Armenia* [2015] ECtHR [GC] 13216/05 [96].

24 Dieter Fleck, 'Occupation' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (Oxford University Press 2021) 298; Cuyckens (n 14) 37; Tristan Ferraro, 'Determining the Beginning and End of an Occupation under International Humanitarian Law' (2012) 94 International Review of the Red Cross 133, 145.

25 Fleck (n 24) 197.

26 The commentary states that '"in the hands of" … simply means that the person is in territory which is under the control of the Power in question'; Jean Pictet and others, *Commentary on the Geneva Conventions of 12 August 1949, Vol IV* (ICRC 1958) 47. See also *Prosecutor v Vinko Martinović and Mladen Naletilić* (Judgment) IT-98-34 (31 March 2003) [208].

27 Pictet and others (n 26) 47.

28 Eliav Lieblich and Eyal Benvenisti, *Occupation in International Law* (Oxford University Press 2023) 221.

29 See also Lubin (n 4) 465.

As shown above, the applicability of IHL norms regulating the exercise of control over a person is delimited mainly in territorial terms. While the collection of data will frequently be effectuated through physical installations (e.g., CCTV) or during physical encounters (e.g., using HIIDE), personal information can be stored and used in any place once transformed into a computer-readable format.[30] This gives rise to a precarious situation: having collected sensitive data while being in physical control of a person or territory, a belligerent party might continue to hold some authority over individual data subjects, even without exercising physical control over them or the territory they are located on.

Thus, data-facilitated control does not fit squarely within the established mechanisms of determining the applicability of those IHL provisions dealing with the exercise of control over an individual as it de-territorializes and compartmentalizes control. The first is due to the virtual nature of data. The second is a consequence of the fact that sensitive data might allow the data holder to exercise significant control over certain aspects of the data subject's life, which nevertheless falls short of complete control over almost all aspects of life a state has when occupying territory.

C. How to Respond to These Challenges?

Does this mean that in the absence of effective control over territory, the law of occupation and the general protections of GCIV would not apply? Not necessarily. At least two avenues leading to the conclusion that IHL will continue to apply to data collected during situations of military control can be identified. While the first would require a novel and thus far unsupported interpretation of Article 4(1) GCIV, the latter has gained prominent scholarly support and could reasonably be extended to the situation discussed in this paper.

D. Interpreting Retaining Personal Data as Remaining in the Virtual Hands of a Belligerent Party

It has been averred that 'taken seriously, the "in the hands" test, as applied to individuals, could perhaps be extended to situations beyond actual physical contact with troops'.[31] Arguing in this vein, one might contend that the prominence of digital means in everyday life has increased to an extent where the term 'person' must be understood as capturing both the physical body of an individual as well as any digital representation thereof. The latter could remain in the hands of a belligerent party even when the physical person is not anymore. This contention relies on the idea that personal data can be conceptualized as a virtual extension of the physical civilian, with the two being linked by the concept of human dignity, which encompasses both physical and non-physical components of the human experience. However, some

30 For instance, portions of the data collected by the US in Afghanistan were reportedly stored on servers in West Virginia; Public Intelligence, 'Identity Dominance: The U.S. Military's Biometric War in Afghanistan' (21 April 2014) <https://publicintelligence.net/identity-dominance/> accessed 14 October 2023.

31 Lieblich and Benvenisti (n 28) 67.

conceptual clarification would be necessary: Would all personal data, such as emails exchanged with a gardening company on the topic of hiring a lawnmower, or only certain especially sensitive categories of data bring a person into the virtual hands of a belligerent party? Moreover, it seems unlikely that courts or states would consider such an approach to constitute *lex lata*.

E. Towards an Extension of the Functional Approach to Personal Data

Some have argued that certain obligations of occupying powers might remain applicable even when the (former) occupying power ceases to exercise effective control.[32] More specifically, if a former occupying power 'retain[s] key elements of authority or other important governmental functions, the law of occupation may continue to apply within the territorial and functional limits of such competences'.[33] While effective control over territory might, therefore, be a necessary condition to *trigger* the applicability of the law of occupation, it might not be required to sustain the applicability of some of its provisions.[34] Some consider this a dangerous fragmentation of the law of occupation, which would create legal uncertainty and 'entrust the occupying power with the ability to determine the extent of its own obligations'.[35] Others argue that without such an approach, a local population might be left 'bereft of any major legal protection' in situations where authority is shared between belligerent states, which stands in stark contradiction with the *telos* of the law of occupation.[36] The post-occupation retention of personal data constitutes one manifestation of such a scenario.

It should be noted that the asymmetry between the test for determining the beginning of the temporal scope of the law of occupation and the test for its end remains undertheorized.[37] Concerning the long-term storage of personal data, this is crucial: If we accept that the law of occupation remains applicable with respect to such data, would we not also have to argue that collecting personal data through purely digital means can trigger the law of occupation in the first place? This would come close to

32 Ferraro (n 24) 157–158; Dinstein (n 23) 301–302; Iain Scobbie, 'An Intimate Disengagement: Israel's Withdrawal from Gaza, the Law of Occupation and of Self-Determination' (2004) 11 Yearbook of Islamic and Middle Eastern Law 3, 30; Aeyal Gross, The Writing on the Wall: Rethinking the International Law of Occupation (Cambridge University Press 2017) 133–134. Note that Gross specifically proposes a functional approach. The other authors advocated for asymmetrical approaches more broadly.

33 International Committee of the Red Cross, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (International Committee of the Red Cross 2015) Report 32IC/15/11 12 <https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts> accessed 22 May 2019.

34 See eg Dinstein (n 23) 301.

35 Cuyckens (n 14) 41–42; Valentina Azarov, 'Disingenuous "Disengagement": Israel's Occupation of the Gaza Strip and the Protective Function of the Law of Belligerent Occupation' (*Opinio Juris*, 24 April 2012) <https://opiniojuris.org/2012/04/24/disingenuous-disengagement-israels-occupation-of-the-gaza-strip-and-the-protective-function-of-the-law-of-belligerent-occupation/> accessed 27 November 2023; Yuval Shany, 'Faraway, So Close: The Legal Status of Gaza after Israel's Disengagement' (2005) 8 Yearbook of International Humanitarian Law 369, 378.

36 Ferraro (n 24) 302.

37 Lieblich and Benvenisti (n 28) 75.

accepting that there can be something like a 'cyber occupation' – an idea that has been prominently and rightly rejected.[38]

However, there are good reasons for this asymmetry. First, IHL is already fragmented regarding the end of its applicability. Indeed, prisoners of war are protected by GCIII 'until their final release and repatriation'.[39] Additional Protocol I (AP I) explicitly states that its applicability extends until the release, repatriation or re-establishment of a person, including after the termination of an occupation.[40] Certain provisions of Additional Protocol II (AP II) apply to individuals deprived of their liberty 'for reasons related to [a] conflict' even if this deprivation begins after the end of the armed conflict.[41] What this implies is that once an armed conflict erupts, IHL applicability mirrors the existence of protective needs. As long as protected individuals are in need of protection as a result of an armed conflict, whether that conflict is ongoing or not, the relevant norms of IHL apply.

Second, a functional approach aligns well with the spirit of the law of occupation. Many would agree that the obligations of an occupying power are the flipside of the authority over foreign people or territory that it exercises during an occupation. The need to have a body of law like the law of occupation emanates from the fact that, as a result of an armed conflict, a belligerent party has gained control over a foreign population, which allows it to impact this population's life in ways that are different from the effects of military attacks. By virtue of the stable control over territory it gained through militarily ousting the previous sovereign, it has created a relationship of dependence between itself and the local population that is not just momentaneous. This fact of the dependence of the local population on the occupying power,[42] without regard for its legitimacy, lies at the heart of the law of occupation. Since it is the occupying power that, for whatever reason, actively decided to create such a dependence, it also bears the responsibility for the effects of actions made possible by this dependence for as long as it decides to maintain it. If it was the fact of having physical control over a person or territory that enabled the creation of a data-facilitated relation of (partial) dependence between the former occupying power and the data subject, it would seem in line with the spirit of the law of occupation that the relevant IHL provisions remain applicable.

Note that if this applies to the provisions of the law of occupation proper, by way of a *maiore ad minus* argument, the same reasoning will apply to the 'in the hands' standard, which arguably requires a lesser level of control. The idea would be similar

38 NATO CCDCOE (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 543.
39 art 4 GCIII.
40 art 3(b) AP I.
41 art 2(3) AP II.
42 Lieblich and Benvenisti (n 28) 78; Yaël Ronen, 'Post-Occupation Law' in Carsten Stahn, Jennifer S Easterday and Jens Iverson (eds), *Jus Post Bellum: Mapping the Normative Foundations* (Oxford University Press 2014) 430–431.

to the one expressed above: as long as there are persons in need of protection as defined by Article 4(1) GCIV, the norms providing protection to such persons in their specific situation remain applicable. Note that this does not create the same outcome as adopting a 'virtual in the hands of' approach. While the former could be interpreted as extending the scope of GCIV to persons who have never been under the physical control of one of the belligerent parties, the functional approach would require the existence of physical control over territory at some point for the initial applicability of the provisions in question to be triggered.

What would this mean in practice? To the extent that there exist relevant IHL provisions, the pertinent rules would govern: (1) the passive storage and (2) the active use or sharing of personal data collected during a belligerent occupation.

4. WHICH NORMS OF IHL WOULD BE RELEVANT?

The question that naturally flows from the previous section is the following: which norms would remain applicable? As this paper is exclusively concerned with determining the applicable law to the post-occupation afterlife of personal data collected by the armed forces, not the application of such norms, this analysis will focus on which rules would be *prima facie* relevant and hence applicable under the functional approach set out above.[43]

A. Rules Related to the Maintenance of Public Order and Security – Article 43 HR

To the extent that data-enabled control allows a foreign state to influence the public order, civil life or security in the former occupied territories, Article 43 HR would be pertinent.

There are two issues to address here. Can the protection of abstract values such as privacy ever be necessary to maintain public order, civil life and security? This will most likely depend on the facts of a specific case. If a data leak or data-facilitated action taken by the occupying power itself was a *sine qua non* condition for social disarray or physical harm to protected persons at the hands of non-state actors, this might, indeed, be considered precisely the kind of outcome that a former occupying

43 Note that this section will not discuss property-related provisions. As suggested in the discussions of the Tallinn Manual experts, the idea that data can be considered property remains a minority position; NATO CCDCOE (n 38) 550. However, should personal data be understood as property by the international community in the future, those provisions dealing with property during belligerent occupation would become further relevant. For a discussion of how to apply the existing property protection rules of IHL to data, *see* Eric Talbot Jensen and Laurie R Blank, 'LOAC and the Protection and Use of Digital Property in Armed Conflict' in Russell Buchan and Asaf Lubin (eds), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (NATO CCDCOE Publications 2022).

power must protect data subjects from, to the extent possible.[44] However, it would be necessary to show that data-enabled conduct actually impacted civil life, public order or security. In the absence of such effects, Article 43 HR will not be pertinent.

A note of caution is in order: considering Article 43 HR pertinent could be interpreted as implying that all Article 43 HR-based positive duties apply – that is, there is a general duty to maintain civil life, public order and security. This would certainly be absurd, as holding personal data gives the former occupying power only very limited control over public order and civil life. Consequently, obligations based on Article 43 HR would be limited to those areas of public order and civil life that can actually be controlled by the occupying power. Unless the occupying power secures very specific data, such as sensitive data on all public servants, it will most likely not be able to control entire areas of public order or civil life. Moreover, it is unlikely that positive obligations would be applicable. However, a case-by-case assessment would be necessary to determine the precise scope of the obligations arising from Article 43 HR.

B. Rules Related to Fundamental Rights of Protected Persons – Article 27 GCIV

An article that would undoubtedly be relevant is Article 27 GCIV. Some have even proposed that the right to privacy could be read into the duty to respect the person, honour and family rights of protected persons.[45] However, the doctrinal permissibility and desirability of such an interpretation are far from obvious. As confirmed by the ICRC commentary on Article 27(1) GCIV, the obligations set out by the provision are absolute and cannot be overridden by security concerns.[46] If one interprets Article 27(1) GCIV to implicitly encompass the right to privacy, then this would either mean that guarantees protected by Article 27(1) GCIV can be limited or that any measure affecting a person's private life was unlawful. The first is a slippery slope, while the second sits uneasily with many provisions allowing for interferences with other rights, such as the right to liberty.[47] To argue that the right to privacy in general is protected in a more absolute manner seems arbitrary. For these reasons, this author is of the view that Article 27(1) GCIV cannot be read as establishing a general right to privacy under IHL.

However, specific uses of data might violate the duty to respect the person and honour of individuals in the hands of a state party. The concept of the *person* has been

44 Note that the International Court of Justice's reference to 'all the measures in [the OP's] power' leaves no doubt that the obligation is one of conduct, not of result; *DRC v Uganda* [2005] International Law Reports 168 (International Court of Justice) 178–179.

45 Talbot (n 6) 835. See also Shehabi (n 6) 98.

46 Pictet and others (n 26) 207; Yutuka Arai-Takahashi, *The Law of Occupation: Continuity and Change of International Humanitarian Law, and Its Interaction with International Human Rights Law* (Brill Nijhoff 2009) 275; Zwanenburg (n 4) 1422.

47 See art 78 GCIV. The ICRC commentary even states that the right to liberty was not included in art 27(1) GCIV precisely because it can be restricted; Pictet and others (n 26) 201.

considered as a broad one that, among other things, encompasses the 'intellectual integrity of human persons'.[48] The ICRC commentary on Article 27(1) GCIV specifies that respect for the intellectual integrity of a person requires that 'individual persons' names or photographs, or aspects of their private lives must not be given publicity'.[49] In light of this, Article 27(1) GCIV can be considered pertinent when data related to the private life of a person, photographs, or names are published, even if this is done after the end of the armed conflict or occupation.

Furthermore, Article 27(1) GCIV is relevant when personal data collected by the former occupying power would put protected persons at risk of violence, insults or threats of either, as well as when it exposes them to public curiosity. A crucial question concerns the precise meaning of the latter term. Does it refer to publishing information in fully public outlets only, or would it also include semi-public spaces (e.g., a shared database accessible to hundreds or thousands of third-party agents)? The ICRC commentary on GCIII states that '"public" should be interpreted as referring to anyone who is not directly involved in handling … prisoners of war, including other members of the Detaining Power'.[50] Whether a similar reasoning applies to Article 27(1) GCIV is one of the questions that will need to be addressed by the forthcoming updated commentary to GCIV, but this author sees no reason why it would not.

C. Rules Related to Specifically Prohibited Practices – Articles 31 and 33 GCIV

The mere threat of publishing sensitive information against the will of the data subject to obtain information from it could amount to moral coercion within the meaning of Article 31 GCIV. As specified in the ICRC commentary, 'the prohibition laid down in this article is general in character and applies to both physical and moral forms of coercion'.[51] Moreover, the pressure exerted can be 'direct or indirect, obvious or hidden'.[52] It is not difficult to imagine a situation where the threat of publishing or sharing sensitive data against the will of the data subject could be used to coerce an individual into sharing certain information. In such a scenario, Article 31 GCIV could provide legal protection.

If the former occupying power were to exercise data-facilitated control (e.g., by publishing or sharing sensitive data) over an entire group, this might further be considered a measure of intimidation or collective punishment pursuant to Article 33(1) GCIV. Note that 'penalties' has been interpreted as not only referring to penal sanctions but to 'penalties of any kind'.[53]

48 Arai-Takahashi (n 46) 271 (fn 37).
49 Pictet and others (n 26) 201.
50 ICRC (n 22) para 1624.
51 Pictet and others (n 26) 219.
52 ibid.
53 ibid 225.

In sum, unless one adopts a very broad interpretation of Article 27(1) GCIV, IHL does not protect privacy as an end in itself. The protection provided by IHL is, therefore, very limited and only shields data subjects from outcomes significantly affecting their dignity or physical or mental well-being, as well as from intimidation, collective punishment or coercion. Therefore, IHL is not necessarily well-suited to protecting the privacy of individuals after the end of a military occupation. Yet, if and to the extent neither IHRL nor domestic data protection laws are applicable, the mostly negative obligations that can be derived from IHL might constitute the only legal safeguards available.

5. CONCLUSION

This paper has explored the question of which legal regimes govern the long-term storage and use of data collected during military occupation. It argued that certain norms of IHL will remain applicable after the end of the occupation. While this author considers this view the most convincing among alternatives, others might reasonably come to different conclusions. This paper argued that as long as IHRL does not apply extraterritorially in situations where a state party has physical control over neither territory nor a person, IHL might provide the only legal safeguard available. If the view that IHRL applies extraterritorially whenever state conduct negatively impacts the enjoyment of rights abroad gains more support, the situation would need to be reassessed. However, so long as this is not the case, IHL will most likely be the only source of international legal restrictions on the retention and use of data collected during a belligerent occupation.

This paper did not seek to explore the applicable substantive norms in full detail. Rather, it is intended to be a conversation starter. While personal data protection might seem like the last thing to worry about in a situation of armed conflict or occupation, and also after it, this sentiment is a dangerous one. Armed conflict increasingly involves the targeting of individual persons as well as the social fabric of societies, including through individual humiliation, discreditation and sowing societal discord. Personal data constitutes one of the most valuable resources in this type of warfare. International lawyers, military and civil-society actors should, therefore, engage in a constructive dialogue on how to protect civilians not only from death, injury and destruction but also from humiliation, intimidation, coercion and other data-facilitated harms, both during and after armed conflict and military occupation.