International Review of the Red Cross (2025), **107** (929), 509–528.
Protection of the Dead
doi:10.1017/S1816383125000165

IRRC

Data and the dead: How does IHL regulate data related to the identification of deceased persons?

Tatjana Grote*
Assistant Lecturer and PhD Candidate,
University of Essex, Colchester, CO4 3SQ, UK
Email: t.grote@essex.ac.uk

Abstract

Data has become central in various activities during armed conflict, including the identification of deceased persons. While the use of data-based methods can significantly improve the efficiency of efforts to identify the dead and inform their families about their fate, data can equally enable harm. This article analyzes the obligations that arise for States regarding the processing of data related to the identification of deceased persons. Despite being drafted long before the "age of data", several international humanitarian law (IHL) provisions can be considered to give rise to obligations which protect those whose data is used to identify the dead from certain data-based harms. However, some of these protections are based on a data protection-friendly interpretation of more general obligations, and many only apply in international armed

* I would like to thank the anonymous reviewers for their very valuable comments and suggestions. Any errors and omissions remain my own. For Kezabu and Oihane.

conflict. Against this background, it is suggested that further analysis on how international human rights law and domestic or regional data protection law could help to strengthen the case for data protection where IHL does not contain specific duties to protect data would be desirable.

Keywords: international humanitarian law, international human rights law, data, deceased persons, identification

: : : : :

Introduction

Data has become essential for both humanitarian and military activities during armed conflict.[1] Most importantly for the purposes of this article, digital methods of data processing, including the use of artificial intelligence, are increasingly being used to identify deceased persons,[2] promising to significantly increase the chances of successful identification.[3] However, as much as it can be a force for good, data can also be an enabler or facilitator of humiliation, coercion, intimidation, discrimination and violence.[4] Privacy scholars have discussed how data can create reputational, emotional, physical, economic and other types of harm during peacetime,[5] and recent years have shown that such harms are at least as pertinent in situations of armed conflict or military occupation.[6] Many humanitarian actors are keenly aware of these risks and have developed detailed guidance and policies on data protection,[7] including with respect to the identification of the dead.[8]

However, it is far less clear which duties arise for States. On the face of it, data protection law might seem like a natural starting point in this respect. Indeed,

1 International Committee of the Red Cross (ICRC) and Privacy International, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, Geneva, October 2018, p. 30.

2 ICRC, *The Forensic Human Identification Process: An Integrated Approach*, Geneva, January 2022, p. 31.

3 Edward Madziwa, "Advancing Honour and Dignity in Death for Victims of Armed Conflicts: Exploring the Challenges and Opportunities of AI and Machine Learning in Humanitarian Forensic Action under IHL", *International Review of the Red Cross*, Vol. 106, No. 926, 2024, pp. 28–29.

4 ICRC, *Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War*, 2nd ed., Geneva, 2021 (ICRC Commentary on GC III), para. 4742.

5 See e.g. Daniel J. Solove and Danielle Keats Citron, "Privacy Harms", *Boston University Law Review*, Vol. 102, No. 3, 2022, pp. 826–859.

6 Although the scenarios discussed below are purely fictional, they are inspired by real-life occurrences of data-based harm during situations of armed conflict or occupation.

7 See e.g. ICRC, *ICRC Rules on Personal Data Protection*, Geneva, 19 December 2019; Office of the United Nations High Commissioner for Refugees, *Policy on the Protection of Personal Data of Persons to Concern of UNHCR*, Geneva, May 2015; Global Privacy Assembly, "Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis Management", October 2020.

8 ICRC/IFRC Family Links Network, *Code of Conduct on Data Protection*, Geneva, November 2015; International Red Cross and Red Crescent Movement, Res. 4, "Resolution on Restoring Family Links while Respecting Privacy, Including as it Relates to Personal Data Protection", UN Doc. 33IC/19/R4, Geneva, December 2019.

data processed to identify the dead will frequently qualify as personal data – i.e., "information relating to an identified or identifiable natural person".[9] In a peacetime setting, such data might be covered by data protection law[10] if such legislation exists,[11] but data protection law will frequently not apply to national security-related conduct[12] or to deceased individuals.[13] More generally, the applicability of domestic law to foreign armed forces in international armed conflict (IAC) and in cases where martial law has been declared is not entirely certain. While data protection law can certainly be highly relevant in some armed conflicts, its applicability and protective value would need to be confirmed on a case-by-case basis.

Consequently, there is merit in turning to the rules of international humanitarian law (IHL) that explicitly regulate the treatment of those who have died in the context of an armed conflict. At the time of the drafting of the most relevant treaties of IHL, digital technologies were not yet invented or were not used as widely as they are nowadays. It is therefore unsurprising that these treaties do not explicitly and comprehensively address certain pertinent issues of data protection. Against this background, the following will provide an initial analysis of how IHL regulates data related to the identification of deceased persons and the harms that might arise from its processing.

For the purposes of this article, data is understood as being related to the identification of deceased persons when it is processed – i.e., collected, shared, retained, disclosed or used – as part of efforts to identify a person who has died in relation to an IAC or a non-international armed conflict (NIAC). This includes both missing person data and unidentified person data.[14] Equally, it covers data relating to the loved ones of a missing person, which is often generated as a by-product in the process of gathering information on a missing person, or is required to inform the loved ones of the fate and whereabouts of their relative.[15] Note that this reflects the intimate connection between the protection of the dead and the rights of the

9 Christopher Kuner and Massimo Marelli, *Handbook on Data Protection in Humanitarian Action*, ICRC, Geneva, 2020, p. 31. Note, however, that certain non-personal data can also create harm, for instance when it allows those viewing the data to make inferences about the ethnicity of a group of persons without relating to a specific individual.

10 Moreover, specific types of harm might be regulated by domestic law (e.g., reputational harms by rules on defamation).

11 The armed conflict in question might take place in a State which does not have a very well-developed or well-enforced data protection law: C. Kuner and M. Marelli, above note 9, p. 28.

12 Robin Geiss and Henning Lahmann, "Protection of Data in Armed Conflict", *International Law Studies*, Vol. 97, No. 1, 2021, p. 568. Note that while this article will occasionally borrow concepts from data protection law, the legal analysis undertaken in the following is not concerned with domestic or regional data protection law.

13 See e.g. 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, [2016] OJ L119, 2016 (General Data Protection Regulation, GDPR), Recital 27. For a general analysis, see Lilian Edwards and Edina Harbinja, "Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World", *Cardozo Arts and Entertainment Law Journal*, Vol. 32, No. 1, 2013, pp. 112–114.

14 ICRC, above note 2, p. 14; Gloria Gaggioli, "International Humanitarian Law: The Legal Framework for Humanitarian Forensic Action", *Forensic Science International*, Vol. 282, January 2018, p. 192.

15 See also ICRC, above note 2, p. 11.

living. Although one important motivation of the rules relating to deceased persons is the protection of their dignity, IHL explicitly states that obligations to facilitate the identification of deceased persons are "prompted mainly by the right of families to know the fate of their relatives".[16] Consequently, the protection of the dead cannot be analyzed in separation from the living whom they leave behind.

It is worth pointing out that efforts to identify the dead and efforts to protect data are not inherently opposed forces. The success of identification will often depend on the availability and quality of data. Where data is not properly protected, it might be deleted or modified (deliberately or accidentally), hence decreasing its availability and quality. Moreover, the loved ones of missing persons might refuse to cooperate due to fears that sharing their personal data could expose them to risks. By sowing such seeds of distrust, insufficient data protection standards can turn into a significant obstacle to achieving humanitarian objectives.[17] Therefore, data protection is generally conducive to the objective of clarifying the fate of missing persons and identifying the dead.[18]

Overall, the article shows that certain rules of IHL can provide protection from various data-based harms, either by outlawing said harms (e.g., dignitary harm arising from the public exposure of deceased persons) or by building protection mechanisms into the default processes relied on in the process of identifying the dead and informing their families about their fate. Moreover, certain more general obligations can be interpreted as giving rise to a duty to prevent data-based harm. However, it should be noted that there is a lack of specific protections in the texts of the relevant treaties, especially in NIAC. It is suggested that the interaction between IHL and international human rights law (IHRL), as well as domestic data protection law with respect to data relating to the dead, should therefore be analyzed further to assess how the latter two bodies of law could complement IHL.

The bright side of data: A brief note on how data can facilitate the identification of deceased persons

As noted by the International Committee of the Red Cross (ICRC), "[i]dentification is achieved through the process of comparison of information".[19] Thus, the identification of the dead is an inherently data-reliant endeavour. To identify a deceased person, two sets of data are needed. On one end, data is collected from an unidentified deceased person (e.g., fingerprints, DNA, dental records, location of body,

16 Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 32.

17 For an example of how a lack of trust in adequate data protection procedures can lead to a refusal to cooperate with or receive the services of humanitarian actors, see "Refugees in Ethiopia's Camps Raise Privacy and Exclusion Concerns over UNHCR's New Digital Registration", *Global Voices*, 19 March 2020.

18 See also Monique Crettol, Lina Milner, Anne-Marie La Rosa and Jill Stockwell, "Establishing Mechanisms to Clarify the Fate and Whereabouts of Missing Persons: A Proposed Humanitarian Approach", *International Review of the Red Cross*, Vol. 99, No. 2, 2018, p. 613.

19 ICRC, above note 2, p. 11.

personal property).[20] On the other end stands data on missing persons (e.g., physical background information, such as sex, age, height, ethnicity or distinct features; and information about a person's social background, such as professional, academic or political affiliation).[21] In the age of social media, data regarding a missing person's last communications and activities can significantly facilitate the process of establishing hypotheses about that person's whereabouts.[22]

The quality and quantity of the available information is a crucial determinant of how likely identification will be, especially in light of the difficulty of ascertaining which information will turn out to be truly relevant at the outset of the identification process.[23] It should be remembered why successful identification is so essential: without it, families will be stuck in a painful limbo between hope and grief – sometimes for years or even decades – which can be likened to a "secret prison".[24] Consequently, there is an understandable incentive to increase the chances of identification as much as possible. This might sometimes translate into collecting as much potentially relevant information as possible. From this perspective, the fact that more and more data is being generated nowadays (e.g., social media, data collected by States or humanitarian actors) can be a source of hope for families who are looking for their lost loved ones.

The dark side of data: How data related to the identification of deceased persons can enable or reinforce harm, and how it is regulated by IHL

As the above has shown, information is central in identifying deceased persons. Yet, as much as data can facilitate the identification of the dead, it can also enable or reinforce harm. The three following fictional scenarios, inspired by real-life events, illustrate this risk. Information-related risks and the harm caused when they materialize are not necessarily new, but as information is increasingly stored and processed in a digital format, they are often magnified due to the increased ease with which the data can be analyzed and shared. Each of the following three scenarios will be followed by an analysis of how the rules of IHL could serve to prevent the relevant data-based harms.

Scenario 1: Respecting the dead in times of social media

In scenario 1, State A is engaged in an IAC with State B and is occupying part of B's territory. As a result of a violent clash between the occupying forces and local insurgents, two civilians die. Soldier S, belonging to State A, takes pictures of the

20 *Ibid.*, pp. 25–26.
21 *Ibid.*, p. 23.
22 *Ibid.*, p. 21.
23 *Ibid.*, p. 23.
24 ICRC, *Accompanying the Families of the Missing: A Practical Handbook*, Geneva, 2013, p. 16.

deceased civilians to facilitate later identification. After uploading said pictures to an unidentified persons database, S also posts them on her public social media accounts, adding a derogatory caption. The picture shows the faces and naked bodies of the two civilians. Soldier S's post goes viral and is viewed by millions of people all around the world.

IHL obligations regarding the respect of the dead

In recent armed conflicts, images of deceased persons have been published online.[25] The above scenario highlights how this can create and magnify dignitary harms caused to deceased persons. It should first be noted that the conduct of soldier S clearly goes beyond the processing which would have been necessary to fulfil the purpose for which the information was initially collected. This is not explicitly and specifically prohibited by IHL,[26] but several rules of IHL do protect the dignity of the dead.

In IAC, Article 34(1) of Additional Protocol I (AP I) obliges States Parties to respect the remains of the deceased. According to the ICRC Commentary on AP I, this includes preventing them "from being exposed to public curiosity".[27] Given that social media content can reach millions of users all over the world, sharing images of the deceased online without anonymizing them first would most certainly qualify as such an act of exposing them to public curiosity. Moreover, Article 16(2) of Geneva Convention IV (GC IV) obliges belligerent parties to protect deceased civilians against ill-treatment.[28] The ICRC Commentary on Geneva Convention II (GC II) states that the concept of ill-treatment should be "interpreted broadly" and

25 See e.g. Suzanne Moore, "Sharing Pictures of Corpses on Social Media Isn't the Way to Bring a Ceasefire", *The Guardian*, 21 July 2014, available at: www.theguardian.com/commentisfree/2014/jul/21/sharing-pictures-corpses-social-media-ceasefire (all internet references were accessed in February 2025); Beena Sarwar, "Social Media Provides Flood of Images of Death and Carnage from Ukraine War – and Contributes to Weaker Journalism Standards", *The Conversation*, 5 August 2022, available at: http://theconversation.com/social-media-provides-flood-of-images-of-death-and-carnage-from-ukraine-war-and-contributes-to-weaker-journalism-standards-181407; Amanda Hess, "The Year in 'Sensitive Content'", *New York Times*, 8 December 2023, available at: www.nytimes.com/2023/12/08/arts/instagram-gaza-israel-children.html.

26 Note that such conduct is contrary to the data protection law principle of "purpose limitation", which requires personal data to only be processed. See e.g. GDPR, above note 13, Art. 1(b). The ICRC Commentaries on the Geneva Conventions refer to certain human rights and soft-law instruments establishing a purpose limitation when discussing when data should not be transmitted to a State Party; see ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces in the Field*, 2nd ed., Geneva, 2016 (ICRC Commentary on GC I), para. 1596; ICRC, *Commentary on the Second Geneva Convention: Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea*, 2nd ed., Geneva, 2017 (ICRC Commentary on GC II), para. 1773.

27 Yves Sandoz, Christophe Swinarski and Bruno Zimmermann (eds), *Commentary on the Additional Protocols*, ICRC, Geneva, 1987 (ICRC Commentary on the APs), para. 1307.

28 While the above scenario involves civilians, note that deceased combatants are protected against despoilment. Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950) (GC I), Art. 15(1); Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950) (GC II), Art. 18(1).

that it certainly includes outrages upon personal dignity and humiliating or degrading treatment.[29] Simply sharing an image of a deceased person, in the absence of any intent or even risk of causing mental suffering or a feeling of humiliation, would not amount to ill-treatment, but due to its humiliating and degrading nature, this author believes that the specific conduct of S would most likely qualify as an outrage upon personal dignity.[30] However, what if the deceased persons in the pictures had not been naked? What if S had not added a derogatory caption? While the concept of ill-treatment remains highly relevant, the uncertainty regarding its precise meaning decreases its immediate utility with respect to conduct falling between the extremes of clearly outrageous behaviour and generally desirable efforts to document atrocities.[31]

Given that the photographs in scenario 1 show deceased civilians in occupied territories, Article 27 of GC IV might regulate the conduct of S more specifically: sharing images of identifiable deceased persons could constitute a failure to protect them against public curiosity, as required by Article 27.[32] However, a crucial question arises: does Article 27 apply to deceased persons?

It has been argued that IHL makes a distinction between protected persons and the dead: had the drafters intended for Article 27 of GC IV to protect deceased persons, they would have explicitly mentioned them.[33] Yet, it is submitted here that this terminological distinction is not as clear-cut as suggested. For instance, Article 139 of GC IV speaks of "protected persons mentioned in Article 136, in particular those who have … died". If a person were to lose their status as a protected person immediately upon death, this formulation would be somewhat contradictory. There are good reasons to believe that this is not just a linguistic lapse, but an expression of the notion that IHL obliges States to protect the dignity of persons beyond their death.[34] Note that if S had taken pictures of dead prisoners of war (PoWs), Article 13(3) of Geneva Convention III (GC III) would be pertinent, and Article 13(3) was considered to be equally applicable to deceased PoWs by the authors of the ICRC Commentary on GC III.[35] There is no reason why this should be any different in

29 ICRC Commentary on GC II, above note 26, para. 1666.

30 For a similar case, see Bundesgerichtshof, *Urteil vom 27. Juli 2017*, Case No. 3 StR 57/17, 27 July 2017. See also Sarah Zarmksy, "Scenario 31: Sharing Degrading Content", *International Cyber Law: Interactive Toolkit*, 18 September 2024, available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_31:_Sharing_degrading_content.

31 See also Sarah Ashbridge, "Digital Dignity in Death: Are the Geneva Conventions Fit for Purpose in the Age of Social Media?", 28 March 2024, available at: https://rusi.org/explore-our-research/publications/commentary/digital-dignity-death-are-geneva-conventions-fit-purpose-age-social-media.

32 This conclusion was reached by the authors of the ICRC Commentary on Geneva Convention III (GC III) with respect to Article 13(3) of GC III ("materials that enable individual prisoners to be identified must normally be regarded as subjecting them to public curiosity"). ICRC Commentary on GC III, above note 4, para. 1627. This author sees no reason why a different interpretation should be adopted for GC IV.

33 Kai Ambos, "Deceased Persons as Protected Persons within the Meaning of International Humanitarian Law: German Federal Supreme Court Judgment of 27 July 2017", *Journal of International Criminal Justice*, Vol. 16, No. 5, 2018, p. 1115.

34 See also E. Madziwa, above note 3, pp. 3–4.

35 ICRC Commentary on GC III, above note 4, para. 1629. Arguing against this conclusion, see William Casey Biggerstaff, "Ukraine Symposium – Photos of the Dead", *Articles of War*, 29 August 2022, available

the case of civilians. Moreover, it should be noted that the Elements of Crimes of the Rome Statute of the International Criminal Court explicitly state that "persons" should be interpreted to include deceased persons in the context of the war crime of outrages upon dignity.[36] As Article 27 of GC IV is equally concerned with the protection of dignity, this author considers it acceptable to consider the general rule of Article 27 as providing protection against being exposed to public curiosity, during life as in death.

By virtue of Article 1 common to the Geneva Conventions (common Article 1) and Article 1 of AP I, belligerent parties are under an obligation to ensure respect for the Geneva Conventions and Additional Protocols by their armed forces as well as by their population as a whole.[37] One might therefore argue that they have a duty to work towards the deletion of such images, which might require regulating online platforms. Since Article 1 of AP I is addressed to all "State Parties", and common Article 1 to all "Contracting Parties", this obligation would arise not just for those engaged in an armed conflict.[38] As States are increasingly regulating online platforms, ensuring respect for the Geneva Conventions and their Additional Protocols with regard to protecting the dignity of the dead should therefore be on the list of regulatory concerns.

However, a careful balance must be struck between protecting the dignity of those seen in the images and other interests. Documenting atrocities can be crucial for criminal investigations and transitional justice purposes,[39] and images of deceased persons on social media could help authorities to clarify the fate of missing persons through open-source investigations,[40] which would be conducive to the right of families to know the fate and whereabouts of their relatives.[41] Therefore, any regulatory action based on the Geneva Conventions or their Additional Protocols should be the result of a careful legislative process of weighing and balancing the

at: https://lieber.westpoint.edu/photos-of-dead/. The author's criticism of the position presented in the ICRC Commentary relates to the question of whether combatants who have died on the battlefield can be considered as "in the hands of" the enemy belligerent party. In the scenario at hand, this argument does not hold since those in occupied territory are clearly "in the hands" of the Occupying Power. Note that the ICRC Commentary on GC I further specifically states that "photographs … taken of the deceased … must not be made public": ICRC Commentary on GC I, above note 26, para. 1662.

36 International Criminal Court, *Elements of Crimes*, Arts 8(2)(b)(xxi) fn. 49, 8(2)(c)(ii) fn. 57.

37 ICRC Commentary on the APs, above note 27, para. 41; ICRC Commentary on GC I, above note 26, para. 150; ICRC Commentary on GC II, above note 26, para. 140; ICRC Commentary on GC III, above note 4, para. 183.

38 ICRC Commentary on the APs, above note 27, paras 41–45; ICRC Commentary on GC I, above note 26, para. 153; ICRC Commentary on GC II, above note 26, para. 140; ICRC Commentary on GC III, above note 4, para. 186.

39 Ed Millet, "Deploying OSINT in Armed Conflict Settings: Law, Ethics, and the Need for a New Theory of Harm", *Humanitarian Law and Policy Blog*, 5 December 2023, available at: https://blogs.icrc.org/law-and-policy/2023/12/05/deploying-osint-in-armed-conflict-settings-law-ethics-theory-of-harm/.

40 Sarah El Deeb, "Investigating War Crimes: Finding the Missing", *Global Investigative Journalism Network*, 5 September 2023, available at: https://gijn.org/resource/reporters-guide-to-investigating-war-crimes-finding-the-missing/.

41 AP I, Art. 32. Note that obligations related to the identification of the dead are also part of customary IHL: Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), Rules 112, 116, available at: https://ihl-databases.icrc.org/en/customary-ihl/rules.

potentially conflicting interests of preserving information conducive to identifying the dead and ensuring the documentation of atrocities, on the one hand, and ensuring the dignity of the dead, on the other. Such a balance might, for instance, take the form of prescribing anonymization measures rather than deletion and defining compelling reasons of public interest that would justify the publication of images in which deceased persons are identifiable.[42] Moreover, content which might facilitate the clarification of the fate of missing persons could be shared with the relevant agencies before being deleted from public platforms.

The previous analysis has focused on IAC. In NIAC, Article 8 of Additional Protocol II (AP II) obliges States Parties to take all possible measures to prevent the dead from being despoiled and to ensure a decent burial.[43] The sentence structure of Article 8 suggests that the explicit protection against ill-treatment which it provides is limited to the wounded, sick and shipwrecked. Moreover, AP II does not provide protection against public curiosity comparable to that of GC IV. Consequently, the treaty-based protection of deceased persons against different forms of adverse treatment is not as far-reaching in NIAC as in IAC.[44] However, it is essential to consider customary law in this respect. State practice shows that several states apply military manuals in NIAC which require their armed forces to respect the dead[45] and protect them from maltreatment.[46] A case-by-case-analysis would be required to ascertain if and under which circumstances these notions would cover the posting of images showing deceased persons. This author would hope that States Parties interpret the pertinent parts of their military manuals in a way that is in line with the International Criminal Tribunal for the former Yugoslavia (ICTY) Appeals Chamber's understanding that "[w]hat is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife".[47]

Scenario 2: Collecting and sharing data

In scenario 2, State C is involved in an armed conflict with neighbouring state D, which is known for its radical laws on non-heterosexual relationships and has publicly executed members of the LGBTQ+ community. Upon a request from D, C

42 For a similar discussion and conclusion, see ICRC Commentary on GC III, above note 4, para. 1627.

43 ICRC Commentary on the APs, above note 27, para. 4656.

44 The ICRC Commentary on Article 8 of AP II explains that it "would not have been realistic" to have the same level of detail regarding the dead and missing as in AP I. However, the Commentary emphasizes the equal importance of informing families about the fate and whereabouts of their relatives and encourages the responsible authorities to try to inform families themselves or facilitate the ICRC's activities in this respect: ICRC Commentary on the APs, above note 27, para. 4657.

45 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 2: *Practice (Part 1)*, Cambridge University Press, Cambridge, 2005, pp. 2663 (Australia), 2664 (Canada, Philippines, New Zealand), 2665 (Spain), available at: https://ihl-databases.icrc.org/en/customary-ihl/practice. Note that Australia even extends all GC IV Art. 27 protections to the remains of all deceased persons, regardless of status before death.

46 See e.g. *ibid.*, pp. 2664 (Ecuador, Nigeria), 2665 (South Africa, UK, US).

47 ICTY, *The Prosecutor v. Duško Tadić*, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction (Appeals Chamber), 2 February 1995, para. 119.

shares information on deceased persons on its territory, including on combatant T who is a national of D and died in combat. Apart from a photo of his military identity disc (or "dog tag"), C transmits a photo of an intimate letter from T's boyfriend, U, found in T's pocket and showing U's current address. A few days later, agents from the "Ministry of Morality" of D appear at U's home and publicly shame him for his presumed romantic relationship with the late T.[48]

IHL obligations on collecting data on unidentified persons

The first question one might ask is whether State C was allowed to record information on T, and especially on the letter he was carrying. Since identification would probably have been possible simply based on his identity disc, was C allowed to also collect the letter from T's boyfriend?

In IAC, Article 16(1) of Geneva Convention I (GC I) and Article 19(1) of GC II oblige belligerent parties to "record as soon as possible, in respect of each … dead person falling into their hands, any particulars which may assist in his identification".[49] A crucial question, however, is *which* information should be collected by States Parties. While certain particulars should always be collected,[50] the formulation "any particulars which *may* assist in his identification"[51] seems to confer on States Parties significant discretion as to the additional information that they can collect. In fact, the ICRC Commentary on GC I even states that "[t]he guiding principle in this area is that as much information as possible that may assist in the identification of the wounded, sick or dead person is to be recorded".[52]

Had T been a civilian who died in detention, then Article 130 of GC IV would have been pertinent. Interestingly, the wording is more precise in this case, narrowing the information to be recorded and shared down to what is "*necessary* for the identification of the deceased internees".[53] Yet another formulation is used in Article 33(2) of AP I, dealing with deceased persons who "would not receive more

48 When armed conflicts are fought along the lines of ethnicity, religion or similar criteria, data might facilitate discrimination. For example, the rollout of a nationwide biometric digital ID system in Ethiopia has been criticized by some for threatening "to embolden ethnic profiling". Zecharias Zelalem, "Ethiopia Digital ID Prompts Fears of Ethnic Profiling", *Reuters*, 1 February 2023, available at: www.reuters.com/article/markets/commodities/feature-ethiopia-digital-id-prompts-fears-of-ethnic-profiling-idUSL8N3470PD/. Similar fears have been expressed by Rohingya refugees: see The Engine Room, *Understanding the Lived Effects of Digital ID: A Multi-Country Study*, January 2020, p. 15.

49 Note that if T had died while detained by C as a PoW, Article 120(2) of GC III would have obliged C to transmit the information collected at the beginning of captivity by virtue of Article 17 of GC III.

50 See GC I, Art. 16(2); GC II, Art. 19(2).

51 GC I, Art. 16(1); GC II, Art. 19(1) (emphasis added).

52 ICRC Commentary on GC I, above note 26, para. 1559. This is in line with the following statement by the ICRC: "No assumptions should be made as to what is 'enough' or 'unnecessary' [at the time of collection], since the value of a piece of information may become clear at a later stage in the process." ICRC, above note 2, p. 23.

53 Emphasis added. This formulation closely resembles the data protection principle of minimization, requiring that personal data be "limited to what is necessary in relation to the purposes for which they are processed": GDPR, above note 13, Art. 5(1)(c).

favourable consideration under the Conventions and [AP I]". With respect to persons who have died in detention, belligerent parties shall record "at least" the information set out in Article 138 of GC IV. However, the ICRC Commentary states that "other *useful* information may be added".[54] For persons within the scope of Article 33(2) of AP I who have died in other circumstances, there is no further specification as to which information should be recorded. Regarding the other side of the information equation, information on missing persons, Article 33(1) of AP I speaks of "all relevant information", which is similarly broad. In IAC as in NIAC, customary IHL compels "each party to the conflict [to] record all *available* information".[55] This formulation seems even broader.

In sum, the wording of provisions detailing which information on deceased persons should be collected differs across different provisions. While the Geneva Conventions contain some guidelines as to which information should definitely be collected,[56] most IHL provisions seem to accord belligerent parties relatively broad discretion when deciding which (additional) information on deceased persons they might want to collect.[57]

The main point of this section is not to argue that the open-ended nature of provisions on the duty to collect information from deceased persons is in itself problematic. A certain degree of flexibility with respect to which information can be gathered from unidentified persons might be necessary, as it is often not entirely clear what kind of information will be most useful in identifying a deceased person[58] and this "may vary considerably in each individual case".[59] Yet, the fact that a great amount of potentially very sensitive personal data related to unidentified persons and their loved ones could be collected by States Parties makes safeguards regarding the sharing and retention of such data all the more important.

IHL obligations on sharing unidentified and missing person data

Inevitably, matching information on missing persons with information on deceased persons so as to identify them requires an exchange of information. As the above scenario suggests, such data transmissions can potentially cause harm. How can IHL provide protection against such harms?

In IAC, National Information Bureaux (NIBs) play a crucial role in organizing and transmitting information.[60] The role of the NIB is to receive information on

54 ICRC Commentary on the APs, above note 27, para. 1250 (emphasis added).

55 ICRC Customary Law Study, above note 41, Rule 116 (emphasis added). Moreover, there is a customary obligation to provide family members of missing persons with "any information … on their [relative's] fate": *ibid.*, Rule 117.

56 See e.g. GC I, Art. 16(2), GC II, Art. 19(2); GC III, Art. 122(4); GC IV, Art. 138; AP I, Art. 33(2)(a).

57 As noted above, Article 130 of GC IV constitutes a notable exception in this respect.

58 ICRC, above note 2, p. 23.

59 ICRC Commentary on the APs, above note 27, para. 1244.

60 Note that States do not always set up NIBs; however, their function is often integrated into existing authorities. ICRC Commentary on GC III, above note 4, para. 4691.

PoWs (including those who have died in captivity)[61] and deceased combatants,[62] as well as on protected persons in the hands of a belligerent party (including those who have died while being interned),[63] and to forward such information. Importantly, for all the previously referenced categories of persons, transmission to the adverse party would be intermediated by the Protecting Power or the Central Tracing Agency (CTA, formerly the Central Prisoners of War Agency).[64] As the CTA is part of the ICRC, data related to deceased persons transmitted through the CTA will be subject to the ICRC's stringent data protection rules, mandating among other things a data protection impact assessment ahead of any further distribution.[65]

While not directly relevant to the scenario at hand, it should be noted that GC IV itself contains certain specific safeguarding duties: where the NIB has reasons to believe that the transmission of information might have a detrimental impact on the person concerned or their relatives,[66] it needs to notify the CTA thereof.[67] However, such concerns are not a valid reason to withhold the information in question from the CTA.[68] The CTA itself is obliged to consider the potential detrimental impact of sharing data and to suspend or adapt the transmission accordingly.[69] This should be highlighted as an example of the timelessness of the Geneva Conventions – even long before the emergence of data-based technologies, as well as the risks and harms associated with them, the drafters integrated a provision that, at least in spirit, somewhat resembles the data protection impact assessments known by modern data protection law.

Interestingly, Article 33(3) of AP I explicitly mentions the possibility of directly transmitting data concerning persons reported missing and requests related thereto to the enemy belligerent party.[70] While the Geneva Conventions do not

61 GC III, Art. 122(7).

62 GC I, Art. 16(3); GC II, Art. 19(3).

63 GC IV, Arts 137, 130(3).

64 ICRC, "The Central Tracing Agency", 2022, available at: www.icrc.org/en/document/central-tracing-agency-reuniting-families-since-1870. Similarly, Article 137 of GC IV obliges the NIB to forward "information concerning protected persons … through the intermediary of the Protecting Powers and likewise through the Central Agency".

65 ICRC Commentary on GC III, above note 4, para. 4842. See also ICRC, above note 7, Art. 22(1)(b); ICRC/IFRC Family Links Network, above note 8, p. 20. Note that where domestic or regional data protection laws exist and the transmission of information on the dead is within their material scope, such provisions might provide protection already at the level of the NIB. However, such domestic rules should not be interpreted in a way which would make transmission to the CTA impossible: ICRC Commentary on GC III, above note 4, para. 4741.

66 In the above scenario, U was not a relative in the strict sense. However, the notion of "relatives" has deliberately not been defined in AP I and might, to the extent practically possible, also include "personal and emotional ties": ICRC Commentary on the APs, above note 27, para. 1215. Moreover, the ICRC Commentary on Article 137 seems to suggest that the concern is, more broadly, "potential prejudice to anyone": Jean Pictet (ed.), *Commentary on the Geneva Conventions of 12 August 1949*, Vol. 4: *Geneva Convention relative to the Protection of Civilian Persons in Time of War*, ICRC, Geneva, 1960, p. 533.

67 GC IV, Art. 137(2).

68 ICRC Commentary on the APs, above note 27, p. 532.

69 GC IV, Art. 140(2); ICRC Commentary on the APs, above note 27, p. 546.

70 Note, however, that Article 33(2) of AP I explicitly states that this does not relieve belligerent parties from the obligation to also send the relevant information to the CTA.

prohibit such direct transmissions, they do establish the above-described intermediated transmission process, together with its safeguarding mechanisms, as the default approach.

However, even when information on civilians[71] protected by GC IV is directly transmitted by the NIB, Article 137(2) of GC IV will still need to be heeded. Strictly speaking, Article 137(2) constitutes an exception to the obligation to transmit potentially harmful information, not an obligation to refrain from doing so. Yet, it would seem in line with the object and purpose of the provision to interpret it as a *de facto* prohibition against transmitting harmful information. This exception is a clear expression of the drafters' intention to mitigate harm to those concerned by the transmitted information. It would be contrary to the object and purpose of the provision to consider that it is within the discretion of each State to decide whether it would nonetheless like to transmit such information directly. However, it should be noted that the State would be always obligated to transmit the information to the CTA.[72]

Apart from the treaty-based rules applicable in IAC, customary law applicable in both IAC and NIAC obliges belligerent parties to "provide [the] family members [of missing persons] with any information … on their fate".[73] The precise modalities of how to transmit such information are not further specified in the identified customary rule.[74] In NIAC, where no specific treaty-based rules on the transmission of information related to dead and missing persons exist, this relative paucity of IHL-based provisions could make domestic data protection law and IHRL potentially essential complementary sources, as will be discussed below.[75]

Applying this to the case of T, the following can be said. The default approach foreseen by the Geneva Conventions would have been to transmit information through the CTA. As the CTA has stringent data protection protocols, the harm to U most likely would have been identified in the risk assessment and mitigated.[76] If T had been a civilian, C's NIB further would have been obliged to alert the CTA to the potential harm that the transmission of information on T could entail. It was argued that the pertinent provision can further be interpreted to outlaw a direct transmission to the adverse party D if such information might cause harm; however, as stated above, data must always be transmitted to the CTA.

71 Moreover, the ICRC Commentary on GC I and GC II suggests that not only the CTA but also the Protecting Powers "would be well advised" to suspend potentially detrimental data transmissions: ICRC Commentary on GC I, above note 26, para. 1597; ICRC Commentary on GC II, above note 26, para. 1774. Similarly, see ICRC Commentary on GC III, above note 4, paras 4736–4737.

72 See ICRC Commentary on GC I, above note 26, para. 1596; ICRC Commentary on GC II, above note 26, para. 1773; ICRC Commentary on GC III, above note 4, para. 4741.

73 ICRC Customary Law Study, above note 41, Rule 117.

74 According to the ICRC Commentary on Article 8 of AP II, "[i]t would not have been realistic to lay down such detailed rules [as in AP I] for the specific circumstances resulting from non-international armed conflicts": ICRC Commentary on the APs, above note 27, para. 4657.

75 This will be discussed further in the next section.

76 See ICRC, above note 7, Art. 22(1)(b). See also ICRC/IFRC Family Links Network, above note 8, p. 20.

Scenario 3: Retaining data

In scenario 3, State E is engaged in a NIAC with non-State armed group F. When activist V goes missing, the authorities invite V's family to provide information on where V was last seen. The family informs the authorities that V was documenting alleged war crimes committed by group F. E records this information in its database on missing persons, which can be accessed without a password from all its military bases. V is identified a few weeks later and her family is informed of her passing. Weeks later, armed forces belonging to F establish control over a military base close to the village in which V's family lives. They later appear at the house of V's family, torture and severely injure her brother. They refer to the data provided by V's family and to V's past activities, for which her family is now being "punished".

IHL obligations on deleting data related to the dead

As mentioned previously, customary IHL establishes an obligation to search for[77] and identify the dead[78] as well as to record all available information on missing people and to provide families with any information on their fate and whereabouts, in both IAC and NIAC. This naturally requires not only the collection, analysis and transmission of data but usually also its retention,[79] thus raising an important question: is there any point at which information relating to the dead must be deleted?

Certainly, the relevant provisions can only be properly complied with if the information in question is retained for as long as necessary to account for the missing, identify the dead and inform their families as required by the norms discussed above. However, there will be a point where information in the hands of a belligerent party might no longer serve any purpose related to the right of families to know the fate and whereabouts of their missing loved ones – e.g., once all information has been transmitted to the CTA, which has thus been enabled to take all the necessary steps. In such a situation, the deletion of data on the dead held by a belligerent party can constitute an important measure to avoid future data-based harm (such as the events described in scenario 3).

IHL itself does not explicitly oblige States Parties to delete the information they hold once it is no longer needed. The updated ICRC Commentary on GC III states that "[o]nce an enquiry has been concluded, all personal information collected with a view to settling the case should be treated in accordance with applicable standards on data protection …, *including, where necessary, deleting or destroying the data*".[80] The Model Law on the Missing states that "[p]ersonal data that has served

77 ICRC Customary Law Study, above note 41, Rule 112.

78 *Ibid.*, Rule 116.

79 See also ICRC Commentary on the APs, above note 27, para. 1271.

80 ICRC Commentary on GC III, above note 4, para. 4761 (emphasis added). See also ICRC, above note 7, Art. 6; ICRC/IFRC Family Links Network, above note 8, pp. 17–18.

the purpose for which it was collected should be deleted or destroyed".[81] In the case of V, having such legislation in place could have prevented significant harm. However, problems might arise where States have no or only very weak data protection standards to this effect, or do not consider their domestic data protection law applicable.

IHL obligations on protecting data related to the dead

In the case of V, harm might have been prevented by having more robust safeguards aimed at protecting the data on the dead and missing that State E held. Beyond the scenario presented above, keeping data safe is crucial.[82]

Again, IHL does not contain an explicit duty to take specific measures to ensure that data is not accessed, interfered with or deleted by malign third parties. The updated ICRC Commentaries on GC I and GC II suggest that the duty to keep data safe is inherent in the requirement to record said information in the first place.[83] This author has great sympathy for the idea of reading data protection considerations into a specific aspect of existing obligations, but others (including States) might consider that such an interpretation veers too far away from the text of the relevant provisions.

In V's case, a similar obligation would need to be read into the customary obligations related to the dead and missing which are applicable in NIAC. If present or future State practice were to show that States apply data protection standards when deciding how to treat data related to the dead after their families have been informed about their relatives' fate, such an interpretation would seem convincing.[84]

It should be noted that F's conduct clearly constitutes a violation of IHL.[85] If there is a foreseeable risk that third-party access to data related to the dead and missing would lead to such a violation, States Parties could have a duty to do everything reasonably in their power to protect such information as part of their general obligation to ensure respect for IHL.[86] A case-by-case assessment would be required to identify when the risk of a violation would be foreseeable and which preventative measures would have been reasonably available.[87] Generally, where data is at risk, emphasizing the responsibility of States Parties to keep data safe could be an additional incentive to comply with their obligation to forward information as quickly as possible.[88] When a State has grounds to believe that it is not in a position to ensure the safety of the personal data that it retains, it can avoid liability for data-enabled

81 ICRC, *Guiding Principles/Model Law on the Missing*, Geneva, 28 February 2009, p. 40.

82 See also ICRC Commentary on GC III, above note 4, para. 4742. Note that the cyber operations targeting the ICRC have shown that there is a very real risk of such data being accessed or otherwise interfered with.

83 ICRC Commentary on GC I, above note 26, para. 1550; ICRC Commentary on GC II, above note 26, para. 1727.

84 Whether this is currently the case lies beyond the scope of this article.

85 Common Art. 3(1)(a); AP II, Art. 4(2)(a)–(b).

86 Common Art. 1; AP I, Art. 1(1). See also ICRC Commentary on GC III, above note 4, paras 187, 197.

87 ICRC Commentary on GC III, above note 4, para. 198.

88 GC I, Art. 16(2); GC II, Art. 19(2); GC IV, Art. 130.

violations by third parties by arranging a transfer of the data it holds to the CTA and destroying its own records once all data has been transmitted. The CTA has the expertise and capacity to store data safely and to conduct data impact assessments.

In sum, IHL does not explicitly specify when or under which circumstances data related to the dead would need to be deleted or how it must be protected. Nonetheless, if the failure to delete data or keep data safe would foreseeably entail a violation of IHL, the general obligation to ensure respect for IHL might serve as a basis for obliging States Parties to take the necessary protective measures. A duty to keep data safe and to potentially delete it has further been read into existing treaty provisions applicable in IAC; a similar approach could be adopted with respect to the customary rules governing the collection and transmission of information on dead and missing persons in NIAC, but such an approach would only be truly convincing if sufficient evidence of State practice supporting it could be adduced.

How IHL could be complemented by other bodies of law: Some preliminary suggestions

As the previous section has shown, some of the rules on the identification of the dead and the right of their families to know about their fate provide explicit protection against certain data-based harms. Others can be interpreted as implicitly establishing certain data protection obligations. However, to provide effective protection in practice, such interpretations would need to be accepted and put into practice by States. Moreover, due to the paucity of treaty-based rules dealing with the identification of the dead in common Article 3 and AP II, reading data protection duties into existing IHL rules appears more difficult in the context of a NIAC. To strengthen the claim that IHL should indeed be interpreted in the suggested manner and to complement its protection, a look beyond IHL might be useful.[89]

International human rights law

Most human rights treaties do not explicitly regulate data.[90] However, the processing of personal data has regularly been considered to fall within the protective scope

89 The following section should not be understood as a conclusive analysis, but rather as sketching out potential areas where further analysis is required.

90 Note that Article 19 of the International Convention for the Protection of All Persons from Enforced Disappearance (ICPPED) specifically regulates personal information related to the search of disappeared persons. Article 19(2) of the ICPPED generally states that the "collection, processing, use and storage of personal information … shall not infringe or have the effect of infringing the human rights, fundamental freedoms or human dignity of an individual". However, the ICPPED is very weakly ratified. Moreover, a fundamental right to data protection has been recognized within the European context, in Article 8 of the European Charter of Fundamental Rights (CFR). Moreover, all members of the Council of Europe have ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), though its material and territorial scope are limited. The CFR only binds EU institutions and EU member States when they are implementing EU law (Art. 51(1)), and Convention 108+ has a broad and flexible exception clause (Art. 3). International Convention for the Protection of All Persons from Enforced Disappearance, 2716 UNTS 3, 20 December 2006 (entered into force 23 December 2010); Charter of Fundamental Rights of the European Union, 2012/C 326/02, 7 December

of the right to private life.[91] The European Court of Human Rights (ECtHR) and the United Nations Human Rights Committee have interpreted said right as establishing five requirements: legality, necessity, proportionality, adequate safeguards and access to remedy.[92] While the precise content of these principles has been analyzed elsewhere,[93] it suffices to say here that the case law on the human right to private life contains certain specific obligations regarding, *inter alia*, the limitation of processing what is necessary for the purpose for which it was collected,[94] ensuring safe storage and transmission,[95] and a limited retention period for personal data.[96]

However, several notes of caution are in order. First, it is not entirely clear to what extent human rights would protect deceased persons.[97] In fact, IHL might provide more direct and complete protection of the dignity of the dead; IHRL would most likely be more useful regarding the protection of information which might cause dignitary, physical, discriminatory or other privacy-based harms to their living relatives. Second, IHRL might not always be applicable. Its precise extraterritorial applicability in situations of IAC remains disputed, and in NIAC, its personal scope might exclude non-State armed groups. Moreover, States can derogate from specific rights, including the right to private life, in times of public emergency.[98] Lastly, although it is by now widely accepted that IHRL does not cease to apply in situations of armed conflict,[99] there is still a great deal of uncertainty as to how exactly IHL and

2000 (entered into force 1 December 2009); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981 (entered into force 1 October 1985).

91 See e.g. *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, UN Doc. A/HRC/27/37, 30 June 2014, para. 20; ECtHR, *S. and Marper v. United Kingdom*, Case Nos 30562/04, 30566/04 (Grand Chamber), 4 December 2008, para. 103.

92 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, Cheltenham, 2022, pp. 468–470.

93 See e.g. Marten Zwanenburg, "The Use of OSINT for Military Operations Abroad under International Humanitarian Law and International Human Rights Law", *Chinese Journal of International Law*, Vol. 23, No. 3, 2024, paras 36–84; A. Lubin, above note 93.

94 ECtHR, *Karabeyoğlu v. Turquie*, Appl. No. 30083/10, 7 June 2016, para. 117.

95 ECtHR, *Weber and Saravia v. Germany (dec.)*, Appl. No. 54934/00, 29 June 2006, para. 95.

96 ECtHR, *Marper*, above note 91, para. 103.

97 Note that the ECtHR has derived protection for the privacy and reputation of the dead from the right to private life of their relatives: see e.g. ECtHR, *M. L. v. Slovakia*, Appl. No. 34159/17, 14 October 2021, para. 23. In favour of human rights being applicable to the dead, see Claire Moon, "Human Rights, Human Remains: Forensic Humanitarianism and the Human Rights of the Dead", *International Social Science Journal*, Vol. 65, No. 216, 2014, p. 58. Moreover, it has been recognized that several human rights "relate to" the protection of the dead: UN General Assembly, *Protection of the Dead*, UN Doc. A/HRC/56/56, 25 April 2024, para. 12.

98 See e.g. European Convention on Human Rights, 213 UNTS 221, 4 November 1950 (entered into force 3 September 1953), Art. 15(1); International Covenant on Civil and Political Rights, 999 UNTS 171, 16 December 1966 (entered into force 23 March 1976), Art. 4(1); American Convention on Human Rights, 22 November 1969 (entered into force 18 July 1978), Art. 27(1).

99 See e.g. International Court of Justice (ICJ), *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004, para. 106; ICJ, *DRC v Uganda*, 19 December 2005, p. 168, para. 216; ECtHR, *Hassan v. United Kingdom*, Case No. 29750/09 (Grand Chamber), 16 September 2014, para. 104; Inter-American Commission on Human Rights (IACHR), *Coard v. United States*, Case No. 10.951, 29 September 1999, para. 41; Human Rights Committee, General Comment No. 31, "The Nature of the General Legal Obligation Imposed on States Parties to the Covenant", UN Doc.

IHRL interact when concurrently applicable. Many seem to agree that IHL and IHRL are, in principle, complementary.[100] This will frequently allow for the avoidance of norm conflicts by interpreting both bodies of law in a coordinated manner.[101]

Without trying to deny these caveats, IHRL could provide useful additional legal "firepower" to "data protection-friendly" interpretations of existing IHL obligations. Although further analysis would be required, such interpretations could be considered as necessary to give effect to the right to private life by harmonizing IHL and IHRL obligations where both are concurrently applicable.

Data protection law

As noted above, some IHL provisions have been interpreted as giving rise to certain data protection obligations. Especially in IAC, international standards would come with the great advantage of ensuring equal protection on all sides, regardless of any differences between the belligerents' data protection laws. Nonetheless, in the absence of comprehensive and well-established international standards, data protection law "proper" could complement the above-identified international protections, providing a stringent, specific and comprehensive legal framework for data processing.

There are three potential caveats to consider here. First, not every country has data protection laws, and for some of those that do, those laws might provide only very limited protection.[102] Second, data protection law can be limited in its applicability to conflict-related activities[103] or where martial law has been declared. Third, not every domestic or regional data protection legislation protects the personal data of the dead.[104] Therefore, certain data-based harms to the dignity of the dead might escape the reach of domestic data protection law.

Generally, it would be problematic if data protection law stood in the way of identifying the dead and informing their families of their fate. In fact, domestic data protection law cannot justify a failure to comply with the obligations arising from

CCPR/C/21/Rev.1/Add.13, 26 May 2004 (General Comment 31), para. 11. See also ICRC Commentary on GC III, above note 4, para. 99.

100 Advocating in favour of conditional or qualified harmonization, see Orna Ben-Naftali and Yuval Shany, "Living in Denial: The Application of Human Rights in the Occupied Territories", *Israel Law Review*, Vol. 37, No. 1, 2004, pp. 103–106; Nancie Prud'homme, "*Lex Specialis*: Oversimplifying a More Complex and Multifaceted Relationship?", *Israel Law Review*, Vol. 40, No. 2, 2007, pp. 364, 390–392. The complementary nature of IHL and IHRL has been emphasized by several judicial and quasi-judicial bodies: IACHR, *Coard*, above note 99, para. 42; IACHR, *Juan Carlos Abella v. Argentina*, Case No. 11.137, Report No. 55/9, 18 November 1997, para. 161; General Comment No. 31, above note 99, para. 8.

101 For an explanation and overview, see Oona A. Hathaway *et al.*, "Which Law Governs during Armed Conflict? The Relationship between International Humanitarian Law and Human Rights Law", *Minnesota Law Review*, Vol. 96, No. 6, 2012, pp. 1897–1899.

102 See above note 13.

103 See above note 14.

104 See e.g. GDPR, above note 13, Recital 27; UK Data Protection Act, 2018, Art. 3. For a comprehensive overview, see L. Edwards and E. Harbinja, above note 13, pp. 112–115.

the pertinent IHL treaties.[105] In many cases, such a failure could be prevented by putting in place procedures and structures to ensure the protection of personal data related to the dead and missing.[106] Depending on the details of the data protection regime in question, however, further adaptations might be necessary to account for the particular humanitarian needs created by armed conflict. For instance, a rigid focus on consent might need to give way to a greater emphasis on the vital interests of the data subject or their relatives and the public interest.[107] Moreover, certain data subject rights (e.g., the right to access or the right to data portability) might need to be limited to account for the realities of armed conflict. A case-by-case analysis would be required to understand how the data protection laws applicable in a specific jurisdiction might need to be adapted.[108]

Conclusion

The processing of data is an integral part of efforts to identify persons who have died in relation to an armed conflict, but data can equally enable or facilitate harm, especially in times of hostilities. Consequently, when harnessing the benefits of the increasing amount of available data, the protection of that data must not be forgotten.

This article has discussed how IHL regulates data related to the identification of deceased persons by analyzing three hypothetical scenarios. The first scenario showed that certain IHL rules can offer protection against the dignitary harm caused to deceased persons (and emotional harm to their families) which can arise when images of their remains are published and disseminated online.

The second scenario revealed that IHL sets a minimum limit, but not a maximum limit, as to which information should be collected from the dead. However, this can be seen as a reflection of the inevitable uncertainty as to which information will be useful in identifying a deceased person. Regarding the transmission of information related to the dead, even before the rise of data and the harms associated with it, the drafters of the Geneva Conventions were concerned with the potential detrimental effects that sharing information on dead and missing people could have.

The third scenario discussed a situation where a failure to keep data safe and to delete it enabled physical harm. IHL does not explicitly contain a duty to delete data related to deceased or missing persons once it is no longer needed, but such a duty could potentially be derived from the general obligation to ensure respect for

105 See Vienna Convention on the Law of Treaties, 1155 UNTS 331, 23 May 1969 (entered into force 27 January 1980), Art. 27. See also ICRC Commentary on GC III, above note 4, para. 4741.

106 ICRC, above note 81, p. 40.

107 ICRC, above note 81, p. 40; Stéphane Kolanowski, "The EU's Contribution to Preserve the IHL Principles Sustaining Impartial Humanitarian Action", in Stephan Marquardt and Steven Blockmans (eds), *The European Union's Contribution to International Peace and Security*, Brill Nijhoff, Leiden, 2023, pp. 299–300. See also GDPR, above note 13, Recital 112.

108 Note that, for instance, the GDPR allows for legislative measures which restrict certain rights and obligations to safeguard, *inter alia*, the rights and freedoms of data subjects or others (which could include the right to know about the fate and whereabouts of one's relatives): GDPR, above note 13, Art. 23(1)(i).

IHL where a failure to delete would foreseeably lead to violations of IHL. Moreover, duties to keep data safe could be read into existing provisions governing IACs.

In sum, IHL outlaws certain data-enabled harms and can be interpreted to oblige States to take certain measures to reduce the risk of other data-based harms. Yet, advancing interpretations ensuring the protection of personal data related to the identification of the dead is easier in IAC than in NIAC. Moreover, even regarding IAC, there is a risk that progressive interpretations which read certain data protection duties into IHL will not be taken up by all States. Generally, IHL-based data protection duties regarding data related to the dead remain somewhat scattered and incomplete. Against this background, it was suggested that the right to private life could strengthen the claim that States are required to protect the data they control. Furthermore, although some adaptations to provide a certain degree of flexibility might be needed, domestic or regional data protection law could complement IHL. However, both approaches come with their own complications and would need to be analyzed further.

As a final remark, it should be said that the protection of data related to the dead should not be seen as a merely theoretical concern. In certain situations, it might be the main determinant of whether those who have lost someone due to armed conflict can grieve as peacefully as possible, or whether they have to fear that the price they pay for identifying their loved ones is losing their own safety and privacy.