International Review of the Red Cross (2025), **107** (928), 2–18.
The Military
doi:10.1017/S1816383124000353

IRRC

What militaries need to know about data protection and the right to digital privacy/private life

Rigmor Argren*
Assistant Professor of Public International Law, School of Behavioural, Social and Legal Sciences, Örebro University, Örebro, Sweden
Email: rigmor.argren@oru.se

Abstract

With the advent of socio-technical systems that gather and process personal data, the capacity to identify and even locate people in an automated fashion has dramatically increased. This article discusses what militaries need to know about data protection and the right to digital privacy/private life when personal data is processed. The focus in this discussion is on sensitive data that makes individuals identifiable. It is here argued that the right to data protection and the right to digital privacy/private life are distinctive and separate rights and should be treated as such, despite some overlaps. Although the law of armed conflict approaches processing of sensitive data in a topical manner, it remains firm on the delimitation between what is permissible and what becomes unlawful when it comes to processing data.

* The author is grateful for the invaluable feedback received on earlier versions of this article from the editors and the anonymous reviewer(s).

This article illustrates that elements of both data protection and protection of the right to privacy/private life can be traced in the law of armed conflict. In fact, both rights remain distinctive also in times of armed conflict and must be separately protected through obligations of result as well as obligations of conduct.

Keywords: armed conflict, right to data protection, right to digital privacy/private life, inherent limitations.

Introduction

New technologies "are extending capabilities beyond the immediate functionality of being able to transmit, store, and process exponentially greater amounts of data".[1] One may speak of a paradigm shift in this regard when the audiovisual surveillance recordings of yesterday are compared with the capabilities of today's technology.[2] Indeed, with the sheer amount of "big data" which can now be quickly processed, data no longer "needs to be 'personalized' in order to identify specific individuals".[3] Throughout the present article, the individual to which the collected or processed data relates will henceforth be referred to as the "data subject", while the data that enables the identification of the individual will be termed "subject data". By definition, such subject data constitutes sensitive data.[4] When compiled and processed en masse, such data creates new value.[5] But "value" must here be understood in a broad sense, beyond monetary revenues – it could encompass "means of state control, cultural production, civil empowerment"[6] or actionable intelligence for law enforcement operations or military interventions.[7]

1 Thomas Philbeck and Nicholas Davis, "The Fourth Industrial Revolution", *Journal of International Affairs*, Vol. 72, No. 1, 2019, p. 18.
2 Human Rights Council, *Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, Including Peaceful Protests*, UN Doc A/HRC/44/24, 25 June 2020, para. 34.
3 Dafna Dror-Shpoliansky and Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – a Proposed Typology", *European Journal of International Law*, Vol. 32, No. 4, 2021, p. 1256.
4 The definition of sensitive data covers more than data which enables identification. Sensitive data can reveal racial or ethnic origin; political opinions and religious or other beliefs, including philosophical; trade union membership; genetic and biometric data; health, sex life or sexual orientation; and criminal offences and convictions. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981, Art. 6.
5 In academic literature, the creation of value from (large) data sets is referred to as datafication. See e.g. Rigmor Argren, "Using the European Convention on Human Rights to Shield Citizens from Harmful Datafication", in Magnus Kristoffersson (ed.), *Proceedings from First Annual FIRE Conference*, Iustus, Uppsala, 2023, pp. 45–46.
6 Ulises A. Mejias and Nick Couldry, "Datafication", *Internet Policy Review*, Vol. 8, No. 4, 2019, p. 3.
7 Fieke Jansen, Javier Sánchez-Monedero and Lina Dencik, "Biometric Identity Systems in Law Enforcement and the Politics of (Voice) Recognition: The Case of SiiP", *Big Data and Society*, Vol. 8, No. 2, 2021, p. 4.

In "an economy driven by the processing of personal data, privacy is related to the control of personal data"[8] – and the increased attention on data protection over the last couple of years has also brought data protection issues to the forefront in the military context, where they constitute fairly new challenges to address.[9] Although the operational implications of data protection primarily pertain to external exposure of combatants' data,[10] this article is focused on the protection of those who are not, or are no longer, taking part in hostilities, and their subject data. For instance, as pointed out by Crawford, there is a considerable amount of subject data that may be collected from prisoners of war (PoWs). Such subject data consists of sensitive data[11] as well as non-sensitive data.[12]

The complexity around the handling of sensitive data seemingly increases exponentially in situations that Lattimer and Sands refer to as "the grey zone", situated between the traditional fields of application of international human rights law (IHRL) and the law of armed conflict (LOAC).[13] Although it has long been firmly accepted in doctrine[14] that many international obligations (such as IHRL) continue to apply in armed conflict, questions of *how* different regimes should be co-applied continue to arise. Co-application may carry practical challenges – and challenges for practitioners. Furthermore, co-application of IHRL and the LOAC in particular prepares the ground for "the potential availability of the jurisdiction of IHRL monitoring bodies"[15] also during armed conflict, which may be perceived as challenging. It goes without saying that *any* co-application of international legal regimes risks creating a norm conflict. It is

8 Carlos Affonso Souza, Caio César de Oliviera, Christian Perrone and Giovana Carneiro, "From Privacy to Data Protection: The Road Ahead for the Inter-American System of Human Rights", in Özgür Heval Çınar and Aysem Diker Vanberg (eds), *The Right to Privacy Revisited: Different International Perspectives*, Routledge, London, 2022, p. 153.

9 Deborah A. Housen-Couriel, "Managing Data Privacy Rights in Multilateral Coalition Operations' Platforms: A 'Legal Interoperability' Approach", in Russell Buchan and Asaf Lubin (eds), *The Right to Privacy and Data Protection in Armed Conflict*, NATO CCDCOE Publications, Tallinn, 2022, p. 230.

10 *Ibid*., p. 233.

11 Subject data for identification consists of "name, rank, date of birth; and any army, regimental, personal or serial number of a POW". Emily Crawford, "The Right to Privacy and the Protection of Data of Prisoners of War in Armed Conflict", in R. Buchan and A. Lubin (eds), above note 9, p. 124. See also Rigmor Argren, "Protection of Biometric Private Life under the European Convention of Human Rights and the Law of Armed Conflict", *Military Law and Law of War Review*, Vol. 62, No. 1, 2024, pp. 82–84.

12 Geneva Convention III promotes collection of data about what items the PoW carried at the time of capture, where the PoW will be housed, what kinds of work they might do in a given day, what kinds and amounts of food they eat, what religion they observe, recording of all their correspondence, and health-related data. See Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950) (GC III), Arts 17, 18, 22, 26, 37, 50–57, 71–76.

13 Mark Lattimer and Philippe Sands (eds), *The Grey Zone: Civilian Protection between Human Rights and the Laws of War*, Hart, Oxford, 2018.

14 See e.g. G. I. A. D. Draper, "The Relationship between the Human Rights Regime and the Laws of Armed Conflict", *Israel Yearbook on Human Rights*, Vol. 1, 1971; Noam Lubell, "Challenges in Applying Human Rights Law to Armed Conflict", *International Review of the Red Cross*, Vol. 87, No. 860, 2005; Marko Milanovic, "A Norm Conflict Perspective on the Relationship between International Humanitarian Law and Human Rights Law", *Journal of Conflict and Security Law*, Vol. 14, No. 3, 2010.

15 Yuval Shany, "Co-application and Harmonization of IHL and IHRL: Are Rumours about the Death of *Lex Specialis* Premature?", in Robert Kolb, Gloria Gaggioli and Pavle Kilibarda (eds), *Research Handbook on Human Rights and Humanitarian Law*, Edward Elgar, Cheltenham, 2022, p. 11.

therefore worth recalling that a norm conflict only exists when a party to "two treaties cannot simultaneously comply with its obligations under both treaties".[16] However, since IHRL and the LOAC "share a common value of protecting human life and dignity",[17] it is here submitted that when it comes to the right to digital privacy/private life, there is no categorical norm conflict between IHRL and the LOAC. Furthermore, concerning the legal protection of subject data, the legal regimes reinforce each other. As this article will illustrate, the complementary differences are found in the *level* of the standard, in certain procedural aspects, and in relation to *contextual* circumstances, but not in relation to the protected values as such.[18] This view aligns with the efforts to counter fragmentation in international law through systemic integration, as indicated in Article 31(3)(c) of the Vienna Convention on the Law of Treaties.[19] For these reasons, the issue of the interaction between IHRL and the LOAC is not further discussed in this article.

This brings us to the primary question addressed by this paper: what do militaries need to know about data protection and the right to digital privacy/private life?[20] The article first considers what distinguishes general data protection from the right to digital privacy/private life.[21] Next, the scope of the human right to digital privacy/private life is outlined. The relevant provisions under the LOAC are then discussed, and matters that militaries need to be

16 Erich Vranes, "The Definition of 'Norm' in International Law and Legal Theory", *European Journal of International Law*, Vol. 17, No. 2, 2006. Compare also the more recent suggestion by Jeutner that "[a] legal dilemma exists when an actor confronts an irresolvable and unavoidable conflict between at least two legal norms so that obeying or applying one norm necessarily entails the undue impairment of the other": Valentin Jeutner, *Irresolvable Norm Conflicts in International Law: The Concept of a Legal Dilemma*, Oxford University Press, Oxford, 2017, p. 20.

17 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), p. 11.

18 It is an illusion that there is only *one* kind of norm conflict. For instance, discussing conflicts of constitutional rights, Croquet points out several kinds of conflict: "an apparent versus an authentic conflict; a horizontal versus a vertical conflict of rights; a vertical versus an artificial conflict of rights; an intra-rights versus an inter-rights conflict; an internal versus an external conflict of rights; and a total versus a partial conflict of rights". Nicolas A. J. Croquet, *The Role and Extent of a Proportionality Analysis in the Judicial Assessment of Human Rights Limitations within International Criminal Proceedings*, Martinus Nijhoff, The Hague, 2015, p. 37.

19 As a general rule of treaty interpretation, States have to take into consideration "any relevant rules of international law applicable in the relations between the parties". Vienna Convention on the Law of Treaties, 1155 UNTS 331, 23 May 1969 (entered into force 27 January 1980), Art. 31(3)(c).

20 Although the rules related to privacy, on the one hand, and private life, on the other, protect the same values, they will remain separated in this paper. The reason for this is first, that they are not identical, and second, that they originate from different legal instruments, which each have their own structure and procedural formulas that impact differently on the respective enforcement and implementation. See, further, below note 46 and accompanying text.

21 As this article is concerned with real-life harms, the normative equivalency paradigm seems sufficiently fitting – that is, "the same human rights that people have offline must be protected online as well". See D. Dror-Shpoliansky and Y. Shany, above note 3, p. 1251. It is noted that this paradigm sees the internet as a tangible sphere, whereas this article remains focused on harms that occur in the real world. See also, generally, the critique directed at this paradigm from the Special Rapporteur on the Right to Privacy in *Report on Security and Surveillance*, UN Doc. A/HRC/37/62, 28 February 2018.

observant about concerning data protection and the right to privacy/private life are raised. Lastly, some conclusions are drawn.

Data protection and protection of digital privacy/private life

In contemporary socio-technical developments, "the very same characteristics of technology that present the greatest opportunities also create the greatest risks".[22] There could be high stakes at play, due to heightened interests in using data in "the commercial/domestic security context".[23] A first matter to consider in terms of the relevant legal regimes in this regard is to distinguish between data protection and the protection of digital privacy/private life as a human right. Therefore, this section first provides a brief overview of existing data protection regimes. Next, the relevant legal provisions of the International Covenant on Civil and Political Rights (ICCPR)[24] and the European Convention on Human Rights (ECHR)[25] are outlined, with a note on derogations. Lastly, similarities and dissimilarities between the respective features of data protection and protection of digital privacy/private life are discussed.

An intricate web of data protection

At the global level, rapid technical development has sparked several initiatives in response to what in essence is modern and intrusive technology. A case in point of such general data protection is the Organisation for Economic Co-operation and Development (OECD) Privacy Framework.[26] But even before the OECD created this framework, the Council of Europe (CoE) had put in place the origins of what is today referred to as Convention 108+.[27]

22 Molly K. Land and Jay D. Aronson, "Technology and Human Rights Enforcement", in Molly K. Land and Jay D. Aronson (eds), *New Technologies for Human Rights Law and Practice*, Cambridge University Press, Cambridge, 2018, p. 126.

23 William H. Boothby, "Biometrics", in William H. Boothby (ed.), *New Technologies and the Law in War and Peace*, Geneva Centre for Security Policy, Geneva, 2019, p. 401.

24 International Covenant on Civil and Political Rights, 999 UNTS 171, 19 December 1966 (entered into force 23 March 1976) (ICCPR).

25 Convention for the Protection of Human Rights and Fundamental Freedoms, 213 UNTS 222, 4 November 1950 (entered into force 3 September 1953) (ECHR).

26 OECD Privacy Framework, 2013, available at: www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en (all internet references were accessed in July 2024).

27 Originally the 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), amended to the modernized Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, as amended 18 May 2018. After the treaty had entered into force, States not members to the CoE were invited to accede to it. As of February 2024, the following non-CoE members are party to the Convention: Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Russian Federation, Senegal, Tunisia and Uruguay. See CoE Treaty Office, "Chart of Signatures and Ratifications of Treaty 108", available at: www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

With a sector-specific approach, the CoE has also regulated the use of personal data in the police sector, pointing out that

> [t]he collection of personal data for police purposes should be limited to such as is necessary for the prevention of a *real* danger or the suppression of a *specific* criminal offence. Any exception to this provision should be the subject of specific national legislation.[28]

Additionally, in 2021, the CoE issued guidelines concerning the use of facial recognition technology (FRT).[29] They stipulate that processing of biometric data requires an appropriate legal basis, including safeguards rooted in domestic law.[30]

In the European Union (EU), the General Data Protection Regulation (GDPR)[31] and EU Directive 2016/680 provide general data protection.[32] The authoritative definitions of these documents have a reach beyond themselves.[33] Article 4(1) of the GDPR defines the data subject as a natural person, either identified or identifiable.[34] As per Directive 2016/680, domestic legislation must operationalize the safeguards stipulated by the GDPR.[35] The same definition of who is a data subject appears in the regulation that applies to EU institutional organs.[36] However, Article 2(2)(d) of the GDPR explicitly excludes the area of

28 Committee of Ministers, Recommendation No. R (87) 15, 17 September 1987, Principle 2.1 (emphasis added).

29 Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Guidelines on Facial Recognition*, 2021, available at: https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751.

30 For an analysis of how this might look under UK domestic law, see Asress Adimi Gikay, "Regulating Use by Law Enforcement Authorities of Live Facial Recognition Technology in Public Spaces: An Incremental Approach", *Cambridge Law Journal*, Vol. 82, No. 3, 2023.

31 Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [GDPR], 27 April 2016.

32 Directive (EU) 2016/680 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data, and Repealing Council Framework Decision 2008/977/JHA, 27 April 2016. For a discussion with an emphasis on the fundamental right to personal data protection under the Court of Justice of the European Union, see, generally, Antonio Reigada Troncoso, "The Principle of Proportionality and the Fundamental Right to Personal Data Protection: The [*sic*] Biometric Data Processing", *Lex Electronica*, Vol. 17, No. 2, 2012, available at: www.lex-electronica.org/en/articles/vol17/num2/the-principle-of-proportionality-and-the-fundamental-right-to-personal-data-protection-the-biometric-data-processing/.

33 A comprehensive analysis of how EU legislation on data protection applies to biometric data within EU-led military missions is given in Sebastian Cymutta, Marten Zwanenburg and Paul Oling "Military Data and Information Sharing – A European Union Perspective", in T. Jančárková, G. Visky and I. Winther (eds), *14th International Conference on Cyber Conflict: Keep Moving*, CCDCOE Publications, Tallinn, 2022.

34 Identifiers can include location data or online identifiers, like internet protocols and cookies. Christopher Kuner, Lee A. Bygrave and Christopher Docksey, "Background and Evolution of the EU General Data Protection Regulation (GDPR)", in Christopher Kuner, Lee A. Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, Oxford, 2020, p. 13.

35 Such regulations may include disclosing biometric data to supranational or intergovernmental organizations, or third States. Sebastian Cymutta, *Biometric Data Processing by the German Armed Forces during Deployment*, CCDCOE Publications, Tallinn, 2022, p. 7.

36 Regulation (EU) 2018/1725 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and

law enforcement. Instead, the relevant framework for data processing in the realm of law enforcement is the Law Enforcement Directive[37] developed alongside the GDPR.

The right to data protection requires the military to create a basic framework which enables concrete accountability for any data processing that is undertaken, be it of sensitive or non-sensitive data. Furthermore, the ambition of the EU data protection law, to harmonize the data protection rules, ought to make data transfers among members of military coalitions easier.[38] Data vulnerabilities which give rise to operational implications ought to be minimized, most notably with regard to "external exposure of combatants' personal data".[39] As for civilians, the GDPR's all-encompassing approach to data should, at least in theory, also cast a regulatory net over non-personalized data, which may still function as an identifier.[40]

Turning to human rights protection, the European Charter of Fundamental Rights[41] has two provisions relevant to digital privacy/private life. Article 7 protects the right to respect for private life, and Article 8(1) separately provides for protection of personal data. This underlines the fact that the right to data protection is distinctive from the right to privacy/private life, and that these two rights should be treated separately, thus distinguishing the European Charter from the general IHRL approach of constructing data protection as a subset of the right to privacy/private life.[42]

A fundamental human right to digital privacy/private life

At the heart of all human rights instruments is the protection of the individual data subject.[43] The Universal Declaration of Human Rights (UDHR)[44] safeguards the right to privacy in Article 12,[45] a provision made enforceable by Article 17 of the

Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002/EC, 2018 O.J. (L 295), 23 October 2018. As noted by Housen-Couriel, this "institutional GDPR" applies when "EU governmental authorities, including military entities, are the data controllers". D. A. Housen-Couriel, above note 9, pp. 240–242.

37 Directive (EU) 2016/680, above note 32.

38 Data sharing among coalition members, including establishing legal interoperability of their activities, is increasingly complex. *Ibid*., p. 229.

39 *Ibid*., p. 233.

40 See above note 3 and accompanying text.

41 Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26 October 2012.

42 Orla Lynskey, "Deconstructing Data Protection: The 'Added-Value' of a Right to Data Protection in the EU Legal Order", *International and Comparative Law Quarterly*, Vol. 63, No. 3, 2014, p. 570.

43 In addition to the treaties discussed in this article, the privacy right has legal protection in the African Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 Rev. 5, 27 June 1981 (entered into force 21 October 1986), Art. 4; the American Convention on Human Rights, 1144 UNTS 123, 22 November 1969 (entered into force 18 July 1978), Art. 11 (reprinted in *Basic Documents Pertaining to Human Rights in the Inter-American System*, OEA/Ser.L.V/II.82 Doc.6 Rev.1, 1992); the ECHR, above note 25, Art. 8; and the Convention on the Rights of the Child, UNGA Res. 44/25, Annex, 20 November 1989 (entered into force 2 September 1990), Art. 16

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

45 *Ibid*., Art. 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

ICCPR.[46] Examining digital privacy under this provision, Lubin discerns five governing principles: (1) The principle of legality, (2) the principle of necessity, (3) the principle of proportionality, (4) the principle of adequate safeguarding, and (5) the principle of access to remedy.[47] These principles can be seen to provide a general framework for what constitutes lawful processing of personal data.

Notably, IHRL has a double focus of protecting the data subject, because it shields the individual both from *actual* harm and also from the *risk* of harm that may foreseeably arise from the processing of subject data. In other words, the focus is on the *purpose* of data processing.[48] This will inevitably entail different kinds of obligations, such as obligations of result (to prevent harm) and obligations of conduct (specified actions to be undertaken in the face of foreseeable risk).[49] The ICCPR protects the right to privacy by shielding the individual from arbitrary or unlawful interference. No specific test is enshrined in the right to privacy under the ICCPR, as is the case with the ECHR, to which we now turn.

The ECHR does not provide an autonomous right to data protection;[50] instead, data protection is addressed as a subset of the right to private life under Article 8.[51] Therefore, despite the increasing scope of what falls under the notion of digital private life, all contemporary processing and handling of subject data will not automatically or categorically come within the ambit of Article 8 or otherwise avail itself of protection by the ECHR[52] – a nexus to at least one of the substantial ECHR rights must be established. On the other hand, when digital private life falls within the ambit of the ECHR, the data subject will be protected from harm and from the *risk* of harm throughout the full data life cycle of collection, retention and disclosure of the subject data by State authorities as well as by private actors. Nor is other data[53] unprotected: if other data makes a person

46 ICCPR, above note 24, Art. 17.

47 For a comprehensive examination of the right to privacy, see Asaf Lubin, "The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law", in R. Kolb, G. Gaggioli and P. Kilibarda (eds), above note 15.

48 For instance, it has been noted that "every individual should have the right to ascertain in an intelligible form, whether and if so, what personal data is stored in automatic data files, and *for what purpose*." Human Rights Committee, CCPR General Comment No. 16, "Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation", 8 April 1988, para. 10, available at: www.refworld.org/docid/453883f922.html.

49 This is not the place to analyze differences between obligations of result and obligations of conduct in detail; suffice it to say that these are not as clear-cut categories as one first may think. See, generally, Rüdiger Wolfrum, "Obligation of Result Versus Obligation of Conduct: Some Thoughts about the Implementation of International Obligations", in Mahnoush H. Arsanjani, Jacob Katz Cogan, Robert D. Sloane and Siegfried Wiessner (eds), *Looking to the Future: Essays on International Law in Honor of W. Michael Reisman*, Martinus Nijhoff, Leiden, 2011.

50 CoE and European Court of Human Rights (ECtHR), "Guide to the Case-Law of the European Court of Human Rights: Data Protection", updated 29 February 2024, p. 7, available at: https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_eng.

51 In addition to private life, the same provision also protects family life, home, and correspondence. ECHR, above note 25, Art. 8(1).

52 CoE and ECtHR, above note 50, p. 7.

53 Other data can for example be employment data, financial data, traffic data, GPS location data and photographs. When assessing other data, a State's margin of appreciation (first referred to in the

identifiable, there is a reasonable expectation of privacy that should be protected.[54] This means that the European Court of Human Rights (ECtHR) may in hindsight scrutinize each phase of the data life cycle by the three-pronged cumulative test to establish if any interference with digital private life (1) was in accordance with the law, (2) was done in pursuance of any of the permissible aims listed, and (3) was necessary in a democratic society.[55] The listed grounds for limitations are national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others.[56] For more than forty-five years, the ECtHR has upheld that there is simply "no room for the concept of implied limitations".[57] Furthermore, in the ECtHR's view, the same standard applies when the management or processing of subject data involves several States. So-called end-to-end protection first requires an assessment of the necessity and proportionality of the data disclosure. Second, from the outset, any bulk interception should be subject to independent authorization.[58] Third, the operation should be subject to supervision and *ex post facto* review.[59] The end-to-end requirement includes clear rules on destruction of incepted data even if no sensitive subject data is present.[60] Pertaining to military operations, "data should be deleted at the latest when the military operation in which the data has been collected ends".[61] There can be no doubt about the ECtHR's position that a State which has the capacity to employ modern technology must accompany such usage with "a simultaneous development of legal safeguards securing respect for citizens' Convention rights".[62]

renowned ECtHR case of *Handyside v. United Kingdom*, Appl. No. 5493/72, Judgment, 7 December 1976, para. 48) can be expected to be wider.

54 ECtHR, *Benedik v. Slovenia*, Appl. No. 62357/14, Final Judgment, 24 July 2018, para. 116.

55 This has also been discussed by Zwanenburg and van de Put with regard to armed forces' use of biometric data. See Marten Zwanenburg and Steven van de Put, "The Use of Biometrics in Military Operations Abroad and the Right to Private Life", in Peter Pijpers, Mark Voskuijl and Robert Beeres (eds), *Towards a Data-Driven Military: A Multi-Disciplinary Perspective*, Leiden University Press, Leiden, 2023, pp. 291–295; R. Argren, above note 11.

56 ECHR, above note 25, Art. 8(2).

57 ECtHR, *Golder v. United Kingdom*, Appl. No. 4451/70, Judgment, 21 February 1975, para. 44. The three-pronged test of the ECtHR will predictably find violations of the right to digital private life if (1) the interference with private life is not necessary in a democratic society, (2) the interference is not the least intrusive available, (3) the data collection seeks to prevent a non-serious offence, (4) the data retention is indefinite, (5) the data retention rules do not separate between (a) sensitive and other data and (b) serious and non-serious offences, (6) there is a lack of or unclear measures against abuse in relation to who can access retained data (sensitive or other), or (7) the data subject has no real possibility of effective legal recourse.

58 With regard to armed forces, it has been pointed out that due to the requirement that the supervision be carried out by authorities independent from those who carry out the surveillance, someone "within the chain of command of the person ordering the use of biometrics … would not be sufficient". M. Zwanenburg and S. van de Put, above note 55, p. 295.

59 ECtHR, *Big Brother Watch and Others v. United Kingdom*, Appl. Nos 58170/13, 62322/14, 24960/15, Judgment (Grand Chamber], 25 May 2021, para. 350.

60 ECtHR, *Centrum för Rättvisa v. Sweden*, Appl. No. 35252/08, Judgment, 25 May 2021, para. 369.

61 M. Zwanenburg and S. van de Put, above note 55, p. 294. Compare also ECtHR, *Cakicisoy and Others v. Cyprus*, Appl. No. 6523/12, Judgment, 23 September 2014, para. 52, where no violation was found, given that destruction of DNA samples was determined to have taken place after the consent forms had expired.

62 ECtHR, *Szabó and Vissy v. Hungary*, Appl. No. 37138/14, Final Judgment, 6 June 2016, para. 68.

Engaging in subject data processing using modern technology without relevant national legislation is simply not an option for a democratic society.

The ECtHR has recently started to grapple with data collection that takes place in real time. In the case of *Glukhin v. Russia*,[63] the applicant complained that there was a violation of his right to private life under Article 8, "following the processing of his personal data in the framework of administrative offence proceedings, including the use of facial recognition technology".[64] The ECtHR held that there had been a violation of the right to private life due to (a) the use of FRT to identify a person conducting a merely administrative offence and (b) the application of FRT in real time to locate and arrest him.[65]

IHRL, unlike the LOAC, permits States to derogate from some rights in specific circumstances.[66] Derogations from human rights treaties primarily remain a domestic matter.[67] Derogations can be used to justify that national legislation is not complied with in full for a specific period of time; in an emergency that "threatens the life of the nation", a State bound by the ECHR could have a legitimate ground to derogate from Article 8. One needs to distinguish, however, between the listed legitimate grounds that already permit interference with the right to digital private life and any measures that are applied following a derogation. A derogation might, at least theoretically, broaden the permissible grounds for interference beyond those explicitly listed as legitimate reasons to infringe on the rights protected by Article 8. Although it is difficult to imagine additional grounds for interference beyond the inherent grounds for limitations (most notably threats to the nation and the protection of public safety and public order), one could assume that a detailed piece of legislation (as required with regard to the collection, retention and disclosure of subject data) might be derogated from when it comes to duration and procedural requirements. As with any derogation, the ensuing interference with the right to digital privacy/private life cannot be entirely unrestricted; it will have to remain in accordance with international law, and any derogation will be subject to legal review under IHRL.

63 ECtHR, *Glukhin v. Russia*, Appl. No. 11519/20, Final Judgment, 4 October 2023.

64 *Ibid*., para. 58. The authorities had used FRT to identify the applicant in a video recording that covered his non-disturbing one-person demonstration outside an underground station: *ibid*., para. 89.

65 *Ibid*., para. 91. Scholars have pointed out that although the ECtHR unanimously found a violation of Article 8 of the ECHR in this particular case, it did not address whether FRT is inherently incompatible with Article 8, and nor did the ECtHR clarify the notions of "general public interest", "public interest" or "national security" that might justify the use of FRT. Francesca Palmiotto and Natalia Menéndez González, "Facial Recognition Technology, Democracy and Human Rights", *Computer Law and Security Review*, Vol. 50, 2023; Monika Zalnieriute, "*Glukhin v. Russia*. App. No. 11519/20. Judgment", *American Journal of International Law*, Vol. 117, No. 4, 2023.

66 For instance, States have frequently derogated in relation to the right of liberty and security and the duration of internments before they are brought before a court. See Françoise Jane Hampson, "Administrative Detention in Non-International Armed Conflicts", in M. Lattimer and P. Sands (eds), above note 13, p. 171.

67 This is discussed in Emilie M. Hafner-Burton, Laurence R. Helfer and Christopher J. Fariss, "Emergency and Escape: Explaining Derogations from Human Rights Treaties", *International Organization*, Vol. 65, No. 4, 2011.

Seeking to disentangle the protective web

Under the GDPR, here seen as a leading regulation for data protection, the subject data is objectified and carries features of commodity,[68] or property.[69] This implies that what is protected is "the process of and efforts to secure and safeguard such digital property from loss, corruption, or compromise, whether inadvertent or due to the nefarious actions of other actors".[70] In addition to finding the balance between data protection and the interests of the free market, the GDPR sets out to ensure that "uniform data protection rules apply in all areas of EU law".[71] With an explicit focus on data, the right to data protection serves to give "individuals more control over more data"[72] compared to what is feasible under the right to privacy/private life. Several differences between data protection and the right to privacy/private life can be discerned. In addition to the obvious differences in application, the object and purpose of these rights are distinctively different. Data protection is primarily concerned with the subject data and seeks to provide the same protective standard to the same kind of subject data across the EU member States. Approaching subject data as an objectified commodity seemingly takes on the character of an obligation of conduct and establishes a framework that theoretically can not only protect subject data from today's processing but also, at least in part, provide protection from socio-technical processing made possible in the future.[73]

By contrast, IHRL maintains a focus on (a) the actual harm and (b) the risk of harm that sensitive data may pose to the data subject. Protecting the data subject from harm is essentially an obligation of result, leaving room for the State to find and apply the most appropriate means and methods. Furthermore, the right to digital privacy/private life within the human rights framework can, if needed, be considered together with additional rights such as freedom of assembly, freedom of movement or the right to life. Additional differences are found in aspects of accountability measures, where the GDPR for instance requires data protection officers.[74] Such structures are designed to provide a remedy for aggrieved

68 The "growing concern regarding the sale of personal data" has been noted by the United Nations General Assembly: see D. Dror-Shpoliansky and Y. Shany, above note 3, p. 1254. The authors cite UNGA Res. A/71/199, "The Right to Privacy in the Digital Age", 19 December 2016.

69 Digital property has been defined as "any information in digital form, whether online or housed in an electronic storage device, [which] can include images, text, sounds, and video". Laurie R. Blank and Eric Talbot Jensen, "LOAC and the Protection and Use of Digital Property in Armed Conflict", in R. Buchan and A. Lubin (eds), above note 9, p. 50.

70 *Ibid.*

71 O. Lynskey, above note 42, p. 572; C. Kuner, L. A. Bygrave and C. Docksey, above note 34, p. 3.

72 O. Lynskey, above note 42, p. 595.

73 This is particularly relevant in relation to systems that use artificial intelligence (AI), due to factors like the speed of technical development, which quickly renders standards obsolete; because AI learns, what was once valid may not be so later on, and as a socio-technical system, AI is highly context-reliant. Thus, what matters is "who uses the technology and for what purpose". Martin Ebers, "Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act", in Larry A. DiMatteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*, Cambridge University Press, Cambridge, 2022, pp. 12–13, available at: http://ssrn.com/abstract=3900378.

74 C. Kuner, L. A. Bygrave and C. Docksey, above note 34, p. 25.

individuals. Nevertheless, it can be challenging for the data subject to prove non-material harm like distress under these regulations.[75] Thus, claiming a violation of the right to digital privacy/private life under IHRL constitutes an additional possible remedy, after domestic remedies have been exhausted.

Turning to the LOAC, two interesting aspects will be revealed. First, provisions relevant for data processing can be noted in the LOAC. Second, and perhaps more interestingly, the distinction between data protection and the right to digital privacy/private life is also noticeable in this legal regime.

LOAC provisions applicable to data protection and digital privacy/private life

Militaries will be well aware of the fact that in an international armed conflict (IAC), the LOAC – consisting of the Hague Regulations,[76] the four Geneva Conventions[77] and, in the case of IAC, Additional Protocol I (AP I)[78] – provides protection of subject data in a manner which must be described as topical. LOAC rules about subject data are predominantly found in provisions that relate to those who are not or are no longer taking part in active hostilities. In other words, rules that explicitly deal with data processing are not first and foremost associated with active hostilities. At the outset, it is essential to note a decisive difference in the geneses of IHRL and the LOAC: human rights treaties are designed to protect the rights of individuals within the jurisdiction of the State Party from arbitrary interference by the State, while the LOAC is, in IAC, designed to protect groups of persons.

International armed conflict and the protection of digital privacy/private life of civilians

In the following paragraphs, two examples of data processing and privacy protection under the LOAC will be presented that arguably mirror data protection and the protection of digital privacy/private life discussed above.

75 A. A. Gikay, above note 30, p. 433.

76 Regulations Respecting the Laws and Customs of War on Land, Annexed to Hague Convention (IV) with Respect to the Laws and Customs of War on Land, 18 October 1907.

77 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); 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); Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950) (GC III); Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) (GC IV).

78 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).

A focus on the processing of sensitive data can be found in Article 34 of Geneva Convention II (GC II).[79] This provision, pertaining to hospital ships, underlines that the mere *possession* of equipment for communication has not been taken as a contravention of the said Article. What matters is what the equipment is used for: "the equipment shall not be used in any circumstances to transmit intelligence data nor in any other way to acquire any military advantage".[80] It is accepted that "due to developments in communication technology, most prominently the use of satellites, encryption is now so common that it is unavoidable as an available technology".[81] With reference to the OECD Privacy Framework,[82] the Commentary on GC II reminds us that due to the right to privacy/private life, all data that is transmitted from hospital ships "must be afforded a reasonable level of security, or a level of security that is commensurate with the sensitivity of such data and the risks involved in their processing".[83] This underlines that data collected from data subjects on hospital ships may only be used for non-hostile purposes. The provision establishes the permissive processing of subject data in a manner that is akin to the data protection laws discussed above.

The other example, pertaining to digital privacy/private life, can be found in Geneva Convention IV (GC IV),[84] which protects civilians who find themselves in the hands of a party to the conflict or Occupying Power of which they are not nationals. The general provision for their protection is found in Article 27, and it ensures the fundamental rights and freedoms of this protected group. The balancing against other interests that may be present in the context appear in the last paragraph of Article 27, which allows States to "take such measures of control and security in regard to protected persons as may be necessary as a result of the war".[85] The balancing here makes no mention of military advantage and clearly concerns protected civilians. Despite the wide discretion afforded to the State in taking measures, such measures "should not affect the fundamental rights of the persons concerned";[86] in other words, the obligation is one of result. The provision explicitly points out that the most severe permissive interference is internment and assigned residence.[87] Therefore, there can be no doubt that anything leading to physical harm of the data subject is prohibited, with no

79 GC II, Art. 34.
80 Louise Doswald-Beck (ed.), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, Cambridge University Press, Cambridge, 1995, para. 171, cited in ICRC Commentary on GC II, above note 17, para. 2402.
81 Bruno Demeyere, Jean-Marie Henckaerts, Heleen Hiemstra and Ellen Nohle, "The Updated ICRC Commentary on the Second Geneva Convention: Demystifying the Law of Armed Conflict at Sea", *International Review of the Red Cross*, Vol. 98, No. 902, 2017, p. 412.
82 See above note 26 and accompanying text.
83 ICRC Commentary on GC II, above note 17, para. 2403.
84 GC IV, Art. 4.
85 *Ibid*., Art. 27.
86 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, 1958, para. 207.
87 GC IV, Art. 27.

exceptions.[88] Furthermore, the explicit prohibition against murdering civilians (and those *hors de combat*) is established as a norm under customary international law in IAC as well as non-international armed conflict (NIAC).[89] This underlines the conclusion that Article 27 of GC IV implicitly presumes the protection of the right to life of the protected persons in question. Without the right to life, there would simply not be any other fundamental rights (including digital privacy/private life) to be concerned about. This customary presumption of protecting the right to life arguably becomes even more important in the context of NIAC.

A note on NIAC, data protection and the protection of digital privacy/private life

It is well known that the rules pertaining to NIACs remain rudimentary. Additional Protocol II (AP II)[90] and Article 3 common to the four Geneva Conventions are the parts of the LOAC that cover NIAC, in addition to those rules that have attained customary law status in NIAC. The problem of a higher threshold for violence that attaches to AP II is well known, as is the fact that AP II, even if ratified by a State, still does not apply to fighting which occurs between armed groups without the involvement of the State, and nor does it apply to State B if it intervenes to support a fight against an armed group (or groups) on the territory of State A.[91]

Additional complications surrounding the applicable LOAC during NIAC relate to the fact that in NIAC there is no equivalent to the combatant status of IAC;[92] the terminology used for those fighting alongside an armed group varies.[93] Nevertheless, a distinction between those fighting and civilians is essential in order to provide civilians with the protection to which they are entitled.[94] This lack of a formal recognition of a group of persons that essentially take active part in NIAC hostilities makes it notoriously difficult to identify members of such groups.[95] If the processing of subject data contributes to or in any other way furthers a status-based labelling, it must be rejected.[96] It is at this point worth

88 *Ibid*., Art. 32.
89 Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005, pp. 311–314, available at: https://ihl-databases.icrc.org/en/customary-ihl.
90 Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II).
91 F. J. Hampson, above note 66, p. 171.
92 For a combatant, taking part in active hostilities is lawful, which means that killing lawful targets, in a lawful manner, will not result in legal consequences after the end of hostilities. AP I, Arts 43, 44.
93 See e.g. Andrew Clapham, *War*, Oxford University Press, Oxford, 2021, pp. 426–427.
94 Nicholas K. Tsagourias and Alasdair Morrison, *International Humanitarian Law: Cases, Materials and Commentary*, Cambridge University Press, Cambridge, 2018, p. 287.
95 Nader I. Diab, Marcos D. Kotlik and Manuel J. Ventura, "Targeting Members of Non-State Armed Groups in NIACs: An Attempt to Reconcile International Human Rights Law with IHL's (De Facto) Status-Based Targeting", in Ezequiel Heffes (ed.), *International Humanitarian Law and Non-State Actors*, Springer, The Hague, 2020, p. 338.
96 Any labelling that can lead to someone being assigned a status as targetable in a conflict should be rejected. *Ibid*.

recalling that the LOAC rules which "[address] direct participation in hostilities are the same in IACs and NIACs. Civilians have legal protection against the effects of hostilities 'unless and for such time as they take a direct part in hostilities.'"[97] As Hampson underlines, for a person to become targetable, s/he has to be *doing* something – it is the *behaviour* that is the determining element, not a status-based labelling, with or without the support of processed subject data.[98] This is not the place to engage in the debates on the scope of direct participation in hostilities and targeting in NIAC, but what can be concluded is that with an emphasis on behaviour, no identification based on the processing of subject data is sufficient to establish that the data subject is a lawful target in NIAC.

Matters to be observant about concerning data protection and the right to digital privacy/private life in operational practice

Although the standard of what data processing of subject data is acceptable will differ between data protection regulations, IHRL and the LOAC, it is essential to remain cognizant of the *purpose* for which the data processing (collection, retention and disclosure) of the subject data is undertaken. Regarding the obligation to only process data for the purpose for which it was originally collected, all the discussed legal regimes converge. As already discussed, the obligation will consist in preventing actual harm as well as foreseeable risk of harm. In the following sections, the two aspects of the purpose of subject data processing and the foreseeable risk in relation to subject data processing are discussed in turn.

Subject data processing for intended purpose only

Data protection laws, IHRL and the LOAC converge with regard to the requirement that subject data can only permissively be used for the purpose for which it was originally intended. Failure to meet this requirement would constitute arbitrariness. Processing of civilians' subject data may under no conditions lead to intentional physical or mental harm to the data subject. The LOAC is firm on this;[99] IHRL, on the other hand, may at first glance appear more flexible in that the right to digital privacy/private life is non-absolute. However, under the ECHR, a detailed three-pronged test is established. Although there is also the possibility (at least in theory) of derogation, it is less clear what additional

97 Françoise Jane Hampson, "Direct Participation in Hostilities and the Interoperability of the Law of Armed Conflict and Human Rights Law", *International Law Studies*, Vol. 87, No. 1, 2011, p. 198 (footnotes omitted).

98 *Ibid*., p. 190. For discussion particularly on "conduct" and "function" in relation to behaviour when determining lawful targeting in NIAC, see, generally, N. I. Diab, M. D. Kotlik and M. J. Ventura, above note 95.

99 See above note 80 and accompanying text.

manoeuvre space a State can gain if it chooses to derogate, given the already inherent and permissible limitations to this right.

The foreseeability of subject data processing causing either harm or risk of harm to the data subject must be considerably higher in the context of armed conflict compared to non-armed conflict situations. At the same time, a higher acceptance of risk is already enshrined in the LOAC, given that it is designed especially for armed conflict, with no additional scope for derogations.

Properly addressing foreseeable risk beforehand

Foreseeable risk means that the State has to take sufficient action beforehand. The *actual* harm is not part of the assessment.[100] When determining if sufficient preventive action has been taken in light of foreseeable risk, three threshold factors have been proposed: (1) the level of harm that may be expected, (2) the likelihood that it will occur, and (3) the level of diligence that is required from the State beforehand.[101] It may well be that this inevitably creates predominantly obligations of conduct. Additionally, since what is examined is the foreseeable risk (rather than the actual harm), the threshold for triggering the preventive obligation is lower, because the task is to anticipate risk.[102] Preventive activities normally include (but are not limited to) ensuring that appropriate legislation and administrative procedures are in place, covering all stages of the full data life cycle, proper planning of any intervention to actively minimize foreseeable risk, ensuring that appropriate equipment is used, and ensuring that adequate training is given beforehand.

In the military context, "responsibility for the intent and the decision rests solely with the commander" in any operation.[103] Data protection rules can of course provide support in decision-making, with the ambition of harmonizing data processing and creating a framework that establishes generic and appropriate procedures and institutions for data handling. Perhaps even more important in relation to foreseeable harm, and the risk thereof, is the notion that a commander's judgemental skill is a learned ability,[104] and that it therefore can – and must – be trained.

To conclude

The three legal regimes discussed in this article give rise to distinctive and overlapping obligations when it comes to the processing of sensitive subject data.

100 Leslie-Anne Duvic-Paoli, *The Prevention Principle in International Environmental Law*, Cambridge University Press, Cambridge, 2018, p. 183.

101 Michael Bothe, "Precaution in International Environmental Law and Precautions in the Law of Armed Conflict", *Goettingen Journal of International Law*, Vol. 10, No. 1, 2020, p. 272.

102 L-A. Duvic-Paoli, above note 100, p. 185.

103 Søren Sjøgren, "What Military Commanders Do and How They Do It: Executive Decision-Making in the Context of Standardised Planning Processes and Doctrine", *Scandinavian Journal of Military Studies*, Vol. 5, No. 1, 2022, p. 392.

104 *Ibid.*

The issue concerns two separate rights and, generally speaking, two kinds of obligations – that is to say, the obligation of result and the obligation of conduct. In this article it has been demonstrated that militaries need to be cognizant of the fact that data protection and the right to digital privacy/private life both merit separate treatment, even though they at times overlap. Furthermore, both rights are protected in non-armed conflict situations and both remain protected should armed conflict erupt. It has been illustrated that also in the LOAC, the right to data protection and a general right to privacy/private life are separately represented. In other words, there is a solid legal framework in place which stipulates that subject data may only be used for the intended purpose. At no stage in the data life cycle (collection, retention and disclosure) is arbitrariness permissible. Using data for aims that deviate from the purpose for which the subject data was collected would constitute such prohibited arbitrariness.

With the common purpose of preventing harm to the data subject, data protection laws, IHRL and the LOAC to varying degrees also address the foreseeable *risk* of harm by data processing at *any* stage in the data life cycle. It has been outlined that due to IHRL's underpinning purpose of shielding people from State intrusion, claiming a violation of the right to digital privacy/private life under, for instance, the ECHR can constitute an additional possible remedy when domestic remedies have been exhausted. It can therefore be concluded that data protection laws, IHRL and the LOAC reinforce each other when it comes to data protection and the protection of digital privacy/private life.

In navigating this complex and intricate web of data protection rules and the right to privacy/private life, it is essential that militaries hold high standards with regard to planning, preparation, selection of equipment and prior training when processing sensitive subject data. Ultimately, this is about the obligation to prevent harm, and additionally to anticipate foreseeable risks attached to any processing of subject data.