The Use of Biometrics in Military Operations Abroad and the Right to Private Life

Zwanenburg, M.; van de Put, S.

DOI
10.24415/9789087284084

Publication date
2023

Document Version
Final published version

Published in
Towards a Data-Driven Military

TOWARDS A DATA-DRIVEN MILITARY

A multidisciplinary perspective

Edited by

Peter B.M.J. Pijpers, Mark Voskuijl, Robert J.M. Beeres

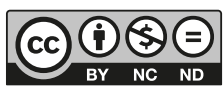
Leiden University Press

The Open Access edition was made possible by a contribution from The Netherlands Defence Academy

Netherlands Annual Review of Military Studies 2022

Cover design: Andre Klijsen
Cover illustration: Media Centre of Defence
Lay-out: Crius Group

ISBN 9789087284084
e-ISBN 9789400604537
https://doi.org/10.24415/9789087284084
NUR 805



CHAPTER 13

The use of biometrics in military operations abroad and the right to private life

Marten Zwanenburg & Steven van de Put

Abstract

This chapter analyses the use of biometrics by military operations extraterritorially from the perspective of the right to private life in Article 8 of the European Convention on Human Rights (ECHR). Such an analysis is called for in view of the increasing use of biometrics by armed forces. The chapter concludes that it follows from the case law of the European Court of Human Rights (ECtHR) that the ECHR is applicable to certain conduct of armed forces outside of their own State's territory, and that this includes situations involving the use of biometrics. Similarly, based on this case law there are good grounds for concluding that all collection, storage and disclosure of biometric data falls within the scope of Article 8 (1) ECHR, at least where the data is systematically collected, stored and shared as is the case in military operations. This means that such use must meet the requirements set out in Article 8 (2) ECHR in order not to constitute a violation of the right to private life. The chapter discusses these requirements and concludes that although States have a certain margin of appreciation, compliance with the right to private life during extraterritorial military operations appears to be a tall order.

Keywords: Biometrics, ECHR, Right to privacy, Jurisdiction, Military operations.

13.1. Introduction

The collection and use of data is an increasingly important feature of military operations. An example of this is the use of biometric systems by armed forces. Biometric systems are systems used for the purpose of the biometric recognition of individuals based on their behavioural and biological characteristics. Such characteristics include fingerprints, face and finger topography, gait, voice and DNA. These characteristics are unique, which makes them ideal for recognising persons. This makes biometric systems a valuable tool for military operations, as they can be used to deny anonymity.

In order for a biometric system to function, it is necessary to collect, store and exchange data. The more data available, the more effective the system is in recognising persons. This has led to the collection of enormous amounts of biometric data in certain recent operations, for example in Afghanistan. This increasing use of biometric systems by military operations raises the question of what the legal parameters are for such use. Only recently has this question been started to be addressed in academic literature. The discussion has mainly focused on the application of International Humanitarian Law (IHL).[1] Thus far, there has been little academic attention for the implications of human rights, in particular the interaction between the right to privacy and the use of biometric data in military operations. Yet the use of data by military operations raises important questions concerning the applicability and application of the right to privacy.

This chapter explores the applicability and application of the right to privacy to the use of biometrics by military operations. It focuses in particular on the right as it has been included in Article 8 of the European Convention on Human Rights (ECHR). This article provides that "Everyone has the right to respect for his private and family life, his home and his correspondence." This choice is motivated by the rich case law of the European Court of Human Rights (ECtHR) concerning the right to private life, as the right to privacy is termed in Article 8 ECHR.

Particular attention will be given in this chapter to the right to private life as it applies to military operations outside of the territory of States. Such extraterritorial operations raise questions concerning the right to private life, including whether that right applies at all outside of such territory. After all, the ECHR was designed to apply primarily in the territory of States Parties. Yet currently it is widely accepted that the application of the ECHR is not limited to the territory of States. This chapter submits that the right to privacy would also be relevant during military operations abroad.[2]

Due to limitations of space, the issue of the interrelationship between the right to private life and IHL during armed conflict will not be explored.[3] It is possible however that the latter may have impact on limitations placed on the use of data by the former.

The chapter is structured as follows. After this introduction, a brief introduction will be given to biometric systems and their use in military operations (section 13.2). Having defined the object of study, section 13.3 will focus on the (extraterritorial) application of the ECHR to military operations. The following section will introduce the right to private life in Article 8 ECHR and discuss the applicability and application of the right to private life to the use of biometric data in military operations abroad. In other words, how does the right to privacy impact such use? (section 13.4). The chapter concludes with a number of final observations and recommendations for further research (section 13.5).

13.2. Biometrics and its use in military operations

An authoritative definition of "biometrics" or "biometric recognition" is that this concerns the automated recognition of individuals based on their biological and behavioural characteristics.[4] A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database.[5] It uses the physical, physiological or behavioural characteristics of individuals to recognise them.[6] Examples of such characteristics are face topography, hand topography, finger topography, iris structure, vein structure of the hand, voice, gait, and DNA.[7] These characteristics are unique, which makes them ideal for recognising persons.[8]

A biometric system can be used for verification or for identification. Verification refers to validating a person's identity by comparing the captured biometric data with his or her own biometric template(s) stored in the system database.[9] This is a one-to-one process, which answers the question of whether the person concerned is who he or she claims to be. Identification refers to recognising an individual by searching the templates of all the users in the database for a match.[10] Identification is a one-to-many comparison to establish an individual's identity, without the person concerned having to claim an identity.

To confirm the identity of individuals, biometric systems make use of various biometric characteristics of individuals that are unique to that individual. This potential, with biometrics representing a unique identifier, makes them very valuable within military operations. It has led to a great number of applications of biometrics in the military domain.[11] Examples of this are base access, identifying persons eligible for host nation training, identifying persons connected to Improvised Explosive Devices (IEDs), identifying persons involved in piracy at sea, and targeting.

The use of biometrics in military operations appears to have been first introduced by the United States (US) after the invasion of Iraq in 2003.[12] The US has taken a leading role when it comes to the use of biometrics, visible in its extensive use during operations in Afghanistan and Iraq. Although the US has remained at the forefront of military use of this technology, other States' armed forces have also started using it during military operations. This is not surprising, considering the broad variety of potential applications referred to above. Currently, NATO has recognised biometrics as an important operational capacity.[13] This highlights that biometrics will be something that is expected to be relevant for the foreseeable future.

13.3. (Extraterritorial) application of the ECHR to military operations

The right to private life in Article 8 ECHR can only be relevant to the use of biometrics by military operations abroad if it applies extraterritorially, i.e. outside of the territory of the State. A key element in this context has always been the concept of jurisdiction. Article 1 of the ECHR provides that "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms" set out in the Convention. This represents 'a threshold criterion which determines whether the state incurs obligations under the treaty, and consequently whether any particular act of the state can be characterised as internationally wrongful.'[14] It is based on the conception that there needs to be a substantial relationship between the State and a potential victim of infringement, to ensure that this relationship is not arbitrary.

As the human rights field matured, courts, including the ECtHR, were increasingly confronted with alleged violations that took place outside a State's own territory. Based on the universal character of human rights, it was argued that it was to be considered arbitrary if States would be allowed to commit violations across their borders.[15] Through a developing jurisprudence it became accepted that whereas 'the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory.'[16] Known as extraterritorial jurisdiction, this meant that States, in certain cases, could also be legally responsible for violations outside of their territory.

Crucial within this notion has been the concept of effective control. This can manifest itself through effective control of territory, or effective control over persons through State agents.[17] Effective control over territory can be exercised either directly by the State through its armed forces, or through a subordinate administration.[18] The case law of the ECtHR also makes clear that there is jurisdiction in the sense of Article 1 ECHR when there is effective control by a State over persons through its agents, which the Court has referred to as "State agent authority and control". This includes, in certain circumstances, the use of force, in particular when an individual is taken into custody.[19] It also includes cases where a State party to the ECHR, through the consent, invitation or acquiescence of the Government of that territory, exercises some or all of the public powers normally exercised by that Government.[20] The precise contours of "State agent authority and control" are however difficult to distil from the ECtHR case law. The Court has however emphasised that the control is actually effective: in situations of chaos,[21] or in situations in which there is an insufficient link between the conduct and the victim[22] the Court has argued against the violation falling within the jurisdiction of the state.

Situations in which a State would hold effective control could thus amount to a sufficient jurisdictional link within operations. Examples relevant to the current

research could include the taking of biometrical data of detainees, in which the individual would without a doubt be seen to fall within the effective control of the State. Individuals aboard a (war-)ship flying the flag of the State could,[23] based on the case law of the ECtHR, also be seen to fall within the control of a state party.

The Court has, however, in applying the notion of effective control to situations of armed conflict, been relatively conservative. In Georgia v. Russia (II), the Court held with regard to Article 2 of the Convention (concerning the right to life) that in the event of military operations carried out during an international armed conflict, it was not possible to speak of "effective control" over an area or over an individual. The very reality of armed confrontation and fighting between enemy military forces seeking to establish control over an area in a context of chaos meant that there could be no such control.[24]

Commentators have noted that this might be due to political concerns and the Court trying to maintain a fine balance between being considered a legitimate court and the compliance of states.[25] Whereas there is legal precedent for arguing that under certain conditions States Parties to the ECHR have effective control through either agents or territorial control, this cannot be presumed.

Recent cases at the Court have however highlighted two relevant factors which would entail that the gathering and also storage of private data could fall within the jurisdiction of a member State. Relevant precedent could be found when considering the Court emphasising close, physical proximity between agents of the State and the victim. A second option would be relying upon the newly established doctrine of "special features" for finding extraterritorial jurisdiction in the sense of Article 1 ECHR, recently employed by the Court when considering a procedural duty to investigate. Whereas both these notions were used by the ECtHR in the context of the right to life, the authors submit that there is no reason in principle why they could not also apply in the context of Article 8 ECHR.

Starting with the concept of proximity, the Court considered this notion in the recent *Carter v. Russia* case, which dealt with the assassination of Alexander Litvinenko by Russian agents in the United Kingdom.[26] In its seminal decision in the case of *Bankovic*, the Court had previously held that the "simple" fact that lethal force was used did not bring an individual within the personal control of a state agent. In *Georgia v. Russia (II)* however, the Court recognised that there had been an evolution in its case law in this respect.[27] It acknowledged that in a number of cases it has applied the concept of "State agent authority and control" over individuals to scenarios going beyond physical power and control exercised in the context of arrest or detention. The Court added that these cases were restricted to situations of 'isolated and specific acts involving an element of proximity'.[28]

Building on this development, in *Carter* the Court considered whether Russian State agents who poisoned Mr. Litvinenko exercised physical power and control

over the life of Mr. Litvinenko. The Court held that this was indeed the case, inter alia because:

> *when putting poison in the teapot from which Mr. Litvinenko poured a drink, they knew that, once ingested, the poison would kill Mr. Litvinenko. The latter was unable to escape the situation. In that sense, he was under the physical control of Mr. Lugovoy and Mr. Kovtun, who wielded power over his life.*[29]

The Court thus looked at whether the Russian agents exercised physical power and control over the life of Mr. Litvinenko, rather than over Mr. Litvinenko as a person. This is an important difference because State agents can impact an individual's rights without having physical control over that individual. It follows from the judgements in *Georgia v. Russia (II)* and *Carter v. Russia* that it is vital that an element of proximity is involved. If this is the case, as was the case in *Carter v. Russia*, it could be argued that the violation 'amounted to the exercise of physical power and control over his life in a situation of proximate targeting.'[30]

Due to the very nature of the gathering of biometric data, this would quite often involve a similar element of proximity. On these grounds, it could be argued that this would fall within the jurisdiction of the State.[31] Examples of this would be the taking of DNA samples, the taking of iris scans or the registration of fingerprints. The gathering of biometric data however does not necessarily involve an element of proximity. Data can also be gathered without involving such an element. This lack of distance however does not necessarily create a fundamental issue for the application of the ECHR.

Here arguments could be presented on the grounds that in the context of the use of biometric data there may be "special features" which bring the situation within the jurisdiction of the State. In a line of case law on the duty to investigate under Article 2 ECHR, the Court has considered that "special features" can also establish a "jurisdictional link" with a State. It remains to be seen whether the Court will also apply the notion of "special features" outside of the context of the procedural obligation to investigate under Article 2 ECHR. If it does, this could provide an additional basis for bringing the use of biometric data within the jurisdiction of the State.[32]

Supporting the notion that the gathering and storage of data could fall within the jurisdiction is the fact that States have so far not contested this notion. Most notably, in the *Big Brother Watch* cases, the Court was directly asked to consider the gathering and storage of data by States. In both cases the respondent State raised no objection to the applicability of the Convention;

> *the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the Government expressly*

> *confirmed that they had raised no objection on this ground as at least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the section 8(4) regime, the matters complained of fell within the jurisdictional competence of the United Kingdom.*[33]

Relying on the *Temple of Preah Vihear* precedent, this silence can also be constructed as legally relevant. In this case, the International Court of Justice (ICJ) held that for any silence to be constructed as legally significant, or as a form of acquiescence, it must be "clear that the circumstances were such as called for some reaction, within a reasonable period."[34] As the ECtHR directly asked (and confirmed) the opinion of the respondent State in these cases, their non-contesting of the fact that the Court found the gathering of data would be within the jurisdiction can be considered legally relevant. It could be seen as a confirmation that the State considers the gathering (and subsequent storage) of personal data outside of their territory to fall within their competence.[35]

The above indicates there are legal arguments for concluding that the gathering and use of biometric data during a military operation by a State outside of its own territory may fall within the jurisdiction of that State. This would make the ECHR relevant, even when this takes place outside of the territory of the State. During military operations, it might thus be the case that the obligations from the ECHR would still apply.

13.4. The right to private life in Article 8 ECHR, its applicability and application to the use of biometric data in military operations abroad

13.4.1. Applicability of the right to private life to the use of biometric data in military operations abroad

The right to privacy, or the right to private life as it is referred to in the ECHR, is laid down in Article 8 ECHR. That article provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The ECtHR has made clear that the "essential object of Article 8 is to protect the individual against arbitrary interference by public authorities."[36] The Court has explained that "private life" is a broad term encompassing the sphere of personal autonomy within which everyone can freely pursue the development and fulfilment of his or her personality and establish and develop relationships with other persons and the outside world.[37] As is clear from the text of Article 8, it first needs to be established whether something constitutes an interference with the exercise of the right to private life. If this is the case, then such interference will constitute a breach of Article 8 if it does not meet the criteria in the second paragraph of the article ("except such as").

This chapter focuses on the use of biometric data in military operations. The first question that needs to be addressed in this context is whether the collection, storage and sharing of biometric data falls within the scope of application of "private life" so that Article 8 is applicable. The case law of the ECtHR makes clear that the storage of information relating to an individual's private life and the release of such information falls within the application of Article 8 (1).[38] In this context, it has underlined that the term "private life" must not be interpreted restrictively.[39]

In Amann v. Switzerland, the ECtHR linked a broad interpretation of the right to privacy in the context of data to international instruments in the field of data protection. It held that such a broad interpretation:

> *corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose is "to secure in the territory of each Party for every individual … respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2).*[40]

This is particularly relevant for biometric data because the use of a biometric system by definition constitutes "automatic processing of personal data".

This case law, and the link it established to the protection of personal data under international data protection instruments, suggest that Article 8 (1) ECHR applies to all collection and further processing of personal data.[41] It would therefore always apply to the collection and further processing of biometric data, which is a particular kind of personal data. This would be particularly so because biometric data is considered a subset of personal data that requires specific protection beyond that provided to "regular" personal data.[42]

This conclusion finds support inter alia in the Grand Chamber judgment in *S. and Marper v. United Kingdom*, in which the Grand Chamber of the ECtHR considered that as fingerprints objectively contain unique information about the

individual concerned, allowing his or her identification with precision in a wide range of circumstances, the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant.[43] The Court continued to hold that:

> *while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constitutes an interference per se with the right to respect for private life.*[44]

Ultimately, whether the collection, storage and sharing of biometric data falls within the scope of Article 8 ECHR needs to be determined on a case-by-case basis. De Vries states that in determining whether this is the case, the ECtHR:

> *Takes into account the specific context in which the information has been recorded and retained, the nature of the records, the way in which they are used and processed, the results that may be obtained and the applicant's reasonable expectations as to the private character of the information.*[45]

The authors consider that there are good grounds for concluding that all collection, storage and disclosure of biometric data falls within the scope of Article 8 (1) ECHR, at least where the data is systematically collected, stored and shared as is the case in military operations. All biometric data objectively contain unique information about the individual concerned, allowing his or her identification with precision in a wide range of circumstances. This means that the rationale given by the Court in *S. and Marper v. UK* for concluding that the retention of fingerprints constitutes an interference per se with the right to respect for private life applies to all biometric data collected, stored and shared in military operations.

13.4.2. Application of the right to private life to the use of biometrics by military operations abroad

1. Requirements in Article 8 (2) ECHR

In the previous section, it was concluded that there are good grounds to conclude that all collection, storage and disclosure of biometric data by a military operation is an interference with the right to private life. Such an interference constitutes a violation of Article 8 ECHR, unless the requirements set out in the second paragraph of that article are met cumulatively. These are that the interference is

a) in accordance with the law;
b) necessary in a democratic society;

c) in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

These requirements are discussed in more detail in this section.

2. Lawfulness

In order not to fall foul of Article 8, the use of biometric data by a military operation must first be "in accordance with the law". This requirement has a formal and substantive sense.[46] In the formal sense, there must be an authorisation by a rule recognised in the national legal order.[47] This prevents the collection, storage and use of this biometric data from being arbitrary and demands a strong legal basis. A number of States have adopted legislation giving their armed forces the power to collect, store and share biometric data. The authors are aware of at least the Netherlands and Germany having such legislation.[48] Such domestic legislation constitutes the "law" referred to in Article 8.

Where such domestic legislation of the State using biometrics abroad is lacking, it may be asked whether domestic legislation of the State where the data is being collected or a resolution of the United Nations Security Council adopted under Chapter VII of the UN Charter can be understood as "law" in the sense of Article 8 (2) ECHR. With regard to the latter, it may be noted that although Article 8 (2) does not specify that "the law" must be domestic law, the ECtHR does refer explicitly to "domestic" law in case law on Article 8.[49] Academic commentaries have however also recognised that a right could potentially be read into some IHL clauses.[50] In a similar fashion, it can be argued that alternative authorisation could be provided by UNSC resolutions. The Court has so far however not considered any international legal or Security Council obligations directly. This can be explained by the fact that the Court has only been asked to consider domestic legislation of the State interfering with the right to privacy. In theory, a host State could also adopt domestic legislation allowing the use of biometrics on its territory by those other States. The ECtHR has not yet addressed the question of whether such legislation could qualify as the "law" under Article 8 (2) ECHR. It has however not excluded this possibility.

The substantive sense of the "in accordance with the law" criterion requires that the rule must be accessible and foreseeable. The ECtHR held in this respect that the:

> *expression "in accordance with the law" further refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned who must, moreover, be able to foresee its consequences for him.*[51]

Foreseeability implies that the law must be sufficiently foreseeable in its terms to give individuals an adequate indication as to the circumstances in which, and the conditions on which, the authorities are entitled to resort to measures affecting their rights under the Convention.[52] If the law grants discretion to public authorities, it must indicate with reasonable clarity the scope and manner of exercise of the relevant discretion so as to ensure to individuals the minimum degree of protection to which they are entitled under the rule of law in a democratic society.[53] In the context of the use of biometrics, albeit not in a military context, the ECtHR has held that:

> *The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed.*[54]

With regard to the requirement that the law is adequately accessible, this means that the person concerned must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. The requirement of accessibility appears to be difficult to meet for the law of the State using biometrics in another State. The very fact that the law is part of another legal system than that of the host State suggests that it is less accessible to persons in the host State. This is all the more so if the law is in a different language than that of the host State.

The requirement in Article 8 ECHR that any interference with the right to private life must be "in accordance with the law" also requires that adequate safeguards be in place to ensure that an individual's Article 8 rights are respected. The law must provide adequate safeguards to offer the individual adequate protection against arbitrary interference.[55] The Court provided some indication of what such safeguards can consist of in its judgment in *S. and Marper v. UK*:

> *It is as essential [...], to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality*[56]

It follows from this requirement that the law providing for the use of biometric data by armed forces will have to provide in some detail when and in respect of whom biometric data can be collected, stored and shared.[57]

3. Necessary in a democratic society

The interference must be "necessary in a democratic society". This means that a fair balance must be struck between the competing interests of the individual and

society as a whole.[58] The interference must correspond to a pressing social need, and, in particular, must remain proportionate to the legitimate aim pursued.[59] This entails an assessment of the proportionality of the interference, i.e. balancing the right of the individual against the interests of the State and the society it represents.[60] Such a balancing will need to be done taking into account the specific circumstances of the case. The ECtHR has held that the requirement of "necessary in a democratic society" must be interpreted narrowly and that the need for restrictions must be convincingly argued in a given case.[61]

In principle, the State has a certain margin of appreciation in determining what it considers necessary in a democratic society.[62] The breadth of the margin varies and depends on a number of factors including the nature of the Convention right at issue, its importance for the individual, the nature of the interference and the object pursued by the interference.[63] In the context of national security, the authorities enjoy a wide margin of appreciation.[64] However, this margin is subject to the supervision of the Court, and the Court must be satisfied that there exist adequate and effective guarantees against abuse.[65] As the ECtHR has held that the need for safeguards to prevent the use of personal data that would be in violation of Article 8 "is all the greater where the protection of personal data undergoing automatic processing is concerned", it appears that the margin of appreciation is more limited in the case of biometric data.[66]

A number of relevant aspects of proportionality can be derived from the case law of the ECtHR. One is that the amount of data that is collected and stored should be as limited as possible.[67] This means that it is unlikely that the large-scale collection and storage of biometric data as was undertaken by the US in Afghanistan would be considered proportional.[68] The data should only be used for the purpose for which it was collected.[69] This means that the sharing of the data by the armed forces with other government agencies in their own State is likely to not be considered proportional. Data should not be kept for longer than is necessary for the purposes for which it has been collected.[70] This implies that normally the data should be deleted at the latest when the military operation in which the data has been collected ends. The data should also be relevant, accurate and up-to-date.[71]

There must also be a system of supervision in place. As the ECtHR held in *Roman Zakharov v. Russia,* it has to determine "whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' to what is 'necessary in a democratic society'".[72] The supervision should normally be carried out by the judiciary. However, the Court has held in the context of secret surveillance that supervision by non-judicial authorities can be sufficient, provided that they are independent of the authorities carrying out the surveillance and are vested with sufficient powers and competence to exercise effective and continuous control.[73] This means that supervision by a person

within the chain of command of the person ordering the use of biometrics in a military operation would not be sufficient. Although supervision by the judiciary is preferred by the ECtHR, it can be argued that at least certain uses of biometrics in military operations, such as when used for intelligence purposes, are similar to secret surveillance and that with regard to such use supervision by a non-judicial authority could meet the requirements of Article 8. Based on publicly available information, however, it appears that there is no independent supervision of the use of biometrics by the armed forces of States Parties to the ECHR.

Closely related to the requirement of supervision is that the individual whose biometric data are used be able to challenge the measure to which he or she has been subjected. A procedure for such a challenge must thus be available.[74]

A second element of the 'necessary within a democratic society' condition is that it is deemed to serve a legitimate purpose. For an interference with the right to private life not to breach Article 8, it must be for one of the purposes referred to in Article 8 (2) ECHR. The ECtHR has interpreted the terms of these purposes rather broadly.[75] Depending on the mandate of the operation, it appears that "national security", "the prevention of disorder or crime" and "the protection of the rights and freedoms of others" would be the most likely legitimate aims for the use of biometrics in a military operation. For example, the use of biometrics in an operation based on national self-defence can contribute to such self-defence, and thereby to the security of the State defending itself. The use of biometrics in an operation aimed at combating piracy, which is an international crime and criminalised as such in the domestic law of most States, can contribute to the prevention of crime. The use of biometrics in an operation supporting another State in fighting a terrorist group can contribute to the protection of the rights and freedoms of others which are threatened by that terrorist group. In such a way the use of biometric data could serve a legitimate purpose within military operations.

13.5. Conclusion

This chapter has demonstrated the relevance of the right to private life in Article 8 of the ECHR during military operations abroad, in particular to the use of biometrics in such operations. It has done so by using a two-pronged approach. In the first section, it has aimed to establish that there are situations in which the use of biometric data abroad could fall within the jurisdiction of a State party to the ECHR. The developing concept of extraterritorial jurisdiction allows for several situations in which a State would be bound to respect the human rights obligations that are relevant for the collection and further processing of biometric data. This is a result of the obligations found within Article 8 of the ECHR. In its case law the ECtHR has established that any

infringement of an individual's privacy may not be arbitrary. States must ensure that any use of biometric data must have a legal basis. Likewise, this must serve a legitimate purpose and be proportionate with regard to the goals of any program. These conditions will still apply to States conducting military operations abroad. Although States have a certain margin of appreciation, compliance with the right to private life during extraterritorial military operations appears to be a tall order. In theory, States may derogate from Article 8, although there is some debate on the possibility of derogation in the context of extraterritorial application of the ECHR.[76] But in any event, derogation is subject to strict limits and therefore is not a panacea.

The appearance of biometric data within doctrines and in the practice of States highlights that its use is here to stay. This makes it necessary to keep conducting research as to the legal framework surrounding this data. This chapter has offered some first considerations on the European perspective towards the human rights obligations that are relevant in these cases. In doing so, it aims to offer a more complete picture surrounding the legal obligations of states when using these new technologies. As technologies and the uses of said technologies keep developing, it remains important to consider the broad range of legal obligations that could potentially influence these uses.

Notes

1 Alison Mitchell, "Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics Notes and Comments," *Canadian Yearbook of International Law* 50 (2012): 289; William H. Boothby "Biometrics" in *New Technologies and the Law in War and Peace*, ed. William H. Boothby (Cambridge University Press, 2019); Rohan Talbot, "Automating occupation: international humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory" *International Review of the Red Cross* 102 (2020): 823; Robin Geiß and Henning Lahmann, "Protection of data in armed conflict" *International Law Studies* 97 (2021): 555; Marten Zwanenburg, "Know thy enemy: the use of biometrics in military operations and International Humanitarian Law" *International Law Studies* 97 (2021: 1403.

2 This application is however still dependent on several conditions which would need to be satisfied.

3 See e.g. Asaf Lubin, "The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law," in *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, eds. Robert Kolb, Gloria Gaggioli and Pavle Kilibarda. Cheltenham: Edward Elgar Publishing, 2022), 463.

4 ISO/IEC International Standard 2382-37, "Information Technology – Vocabulary – part 37: biometrics 2" (2012).

5 Anil Jain, Arun Ross, Salil Prabhakar, "An introduction into biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology* 14 (2004): 4, 5.

6 See for an extensive description of biometrics inter alia Nancy Y. Liu, *Bio-privacy: Privacy Regulations and the Challenge of Biometrics.* Milton Park, Abingdon, Oxon; New York: Routledge, 2012, 29–59.

7 For additional characteristics see Boothby, *supra* note 1, p. 192.

8 "Recognising" is used here as a term encompassing verification and identification as defined below.

9 Jain et al, "An Introduction into Biometric Recognition," 5.

10 Jain et al, "An Introduction into Biometric Recognition," 6.

11 See e.g. William Buhrow, *Biometrics in Support of Military Operations: Lessons from the Battlefield* (Boca Raton: CRC Press, 2017) 41–68.

12 Buhrow, *Biometrics in Support of Military Operations*, 3.

13 Mark Lunan, "New Doctrinal Concepts: Biometrics," *The Three Swords Magazine* 33 (2018): 37.

14 Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* Oxford: Oxford University Press, 2011, 46.

15 See e.g. Issa and Others v. Turkey, no. 31821/96, § 71, 16 November 2004.

16 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 883, 9 July 2004, para. 109.

17 Al-Skeini and Others v. the United Kingdom [GC], no. 55721/07, 7 July 2011, para. 130-140.

18 See e.g. M.N. and Others v. Belgium (decision) [GC], no. 3599/18, 5 May 2020, para. 103; Sandu and Others v. the Republic of Moldova and Russia, nos. 21034/05 and 7 others, 17 July 2018, paras. 36-38.

19 Al Skeini and others v. United Kingdom, para. 136.

20 Al Skeini and others v. United Kingdom, para. 135.

21 Georgia v. Russia (II) [GC], no. 38263/08, 21 January 2021.

22 See e.g. Banković and Others v. Belgium and Others (decision) [GC], no. 52207/99, 12 December 2001.

23 See e.g. Medvedyev and Others v. France, no. 3394/03, 10 July 2008.

24 Georgia v. Russia (II), paras. 126, 137. For a discussion of this judgment see Floris Tan and Marten Zwanenburg, "One step forward, two steps back? *Georgia v Russia (II)*, European Court of Human Rights, Appl No 38263/08," *Melbourne Journal of International Law* 22 (2021): 136.

25 Marko Milanovic, "Al-Skeini and Al-Jedda in Strasbourg," *European Journal of International Law* 23 (2012): 121.

26 Carter v. Russia, no. 20914/07, 21 September 2021.

27 Georgia v. Russia (II), para. 114.

28 Georgia v. Russia (II), para. 132.

29 Carter v. Russia, para. 160.

30 Carter v Russia, para. 161.

31 One of the crucial questions for the court to consider would thus be if the gathering of data took place with an element of proximity or through a more remote method. This could influence if the Court would consider this to fall within a state's jurisdiction. See; Marko Milanovic, "European Court Finds Russia Assassinated Alexander Litvinenko," EJIL:Talk!, September 23, 2021. https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.

32 See for a further explanation of special features: Eugénie Delval, "The Kunduz Airstrike before the European Court of Human Rights: a glimmer of hope to expand the Convention to UN Military Operations, or a tailored jurisdictional link?" *The Military Law and the Law of War Review* 59 (2021): 244, 256-258.

33 Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021, para. 272.

34 Case concerning the Temple of Preah Vihear (Cambodia v. Thailand) (judgement) [1962] ICJ Rep 260, 15 June 1962, para 23.

35 Whereas beyond the scope of this chapter, the Court seems to consider that this would also be the case when receiving data from third parties. See; Big Brother Watch and Others v. the United Kingdom, paras. 495-497.

[36] See e.g. P. and S. v. Poland, no. 57375/08, 30 October 2012, para. 94.

[37] Jehova's Witnesses of Moscow v. Russia, no. 302/02, 10 June 2010, para. 117.

[38] Leander v. Sweden, Series A no. 116, 26 March 1987, para. 48; Rodica Mihaela Rotaru v. Romania, no. 34325/05, 10 November 2009, para. 43.

[39] Amann v. Switzerland [GC], no. 27798/95, 16 February 2000, para. 65.

[40] Amann v. Switzerland, para. 65. See also Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, 27 June 2017, para. 133.

[41] David Harris, Michael O'Boyle, Ed Bates and Carla Buckley, *Law of the European Convention on Human Rights.* Oxford: Oxford University Press, 2018, 524. But see also Kokott and Sobotta, who suggest that the protection of Article 8 ECHR only starts to apply as an event recedes into the past. Juliane Kokott and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3 (2013): 222, 224.

[42] See e.g. Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and to the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[43] S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008.

[44] S. and Marper v. the United Kingdom, para. 86.

[45] Karin de Vries, "Right to Respect for Private and Family Life," in *Theory and Practice of the European Convention on Human Rights*, eds. Pieter van Dijk, Fried van Hoof, Arjen van Rijn and Leo Zwaak. Cambridge, Antwerp, Portland: Intersentia, 2018, 667, 673.

[46] Wiliam Schabas, *The European Convention on Human Rights: A Commentary.* Oxford: Oxford University Press, 2015, 402.

[47] Schabas, *The European Convention on Human Rights*, 402.

[48] See for the Netherlands the Uitvoeringswet Algemene Verordening Gegevensbescherming and the Regeling Gegevensbescherming Militaire Operaties. For Germany see e.g. Sebastian Cymutta, "Biometric Data Processing by the German Armed Forces during Deployment," *NATO CCDCOE Research Paper* (2021): 9-12

[49] See e.g. S. And Marper v United Kingdom, para. 95.

[50] See Zwanenburg, "Know Thy Enemy".

[51] Klaus Müller v. Germany, no. 24173/18, 19 November 2020, para. 49.

[52] Fernández Martínez v. Spain, no. 56030/07, 15 May 2012, para. 117.

[53] Piechowicz v. Poland, no. 20071/07, 17 April 2012, para. 212.

[54] S and Marper v. United Kingdom, para. 96.

[55] Bykov v. Russia [GC], no. 4378/02, 10 March 2009, para. 81.

[56] S. and Marper v. United Kingdom, para. 99.

[57] It has been argued that the domestic legislation of the Netherlands does not meet this requirement. See Jeanice Koorndijk, "De Verwerking van Biometrische Gegevens tijdens Stability-policing-operaties van de Nederlandse Krijgsmacht: Richting Lessons Learned ter Verbetering van het Juridisch Kader" (Master's thesis, University of Amsterdam, 2021), 33.

[58] Keegan v. Ireland, Series A no. 290, 26 May 1994, para. 94.

[59] See e.g. Vavřička and Others v. the Czech Republic [GC], nos. 47621/13 and 5 others, 8 April 2021, para. 273.

[60] Schabas, *The European Convention on Human Rights: A Commentary,* 406.

[61] See e.g. M.N. and Others v. San Marino, no. 28005/12, 7 July 2015, para. 73.

[62] Schabas, *The European Convention on Human Rights: A Commentary,* 406. See generally on the margin of appreciation in the context of Article 8 Yutaka Arai, "The Margin of Appreciation Doctrine

in the Jurisprudence of Article 8 of the European Convention on Human Rights," *Netherlands Quarterly of Human Rights* 16 (1998): 41.

63 S. and Marper v. United Kingdom, para. 102.

64 Big Brother Watch and others v. United Kingdom, para. 338.

65 Klass and Others v. Germany, Series A no. 28, 6 September 1978, para. 50.

66 M.K. v. France, no. 19522/09, 18 April 2013, para. 35.

67 See e.g. Catt v. the United Kingdom, no. 43514/15, 24 January 2019, para. 123.

68 See for a brief description of the large-scale collection in Afghanistan e.g. Katja Linskov Jacobsen, "Biometric data flows and unintended consequences of counterterrorism," *International Review of the Red Cross* 103 (2021): 619, 626.

69 See e.g. Karabeyoğlu v. Turkey, no. 30083/10, 7 June 2016, para. 117.

70 See S. and Marper v. United Kingdom, para. 103.

71 See e.g. M.K. v France, para. 36; Khelili v. Switzerland, no. 16188/07, 18 October 2011, paras. 64-70.

72 Roman Zakharov v. Russia [GC], no. 47143/06, 4 December 2015, para. 232.

73 Klass and others v. Germany, para. 56.

74 See e.g. Vig v. Hungary, no. 59648/13, 14 January 2021, para. 57; Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016, para. 86; M.N. and others v. San Marino, para. 78.

75 Schabas, *The European Convention on Human Rights: A Commentary,* 405.

76 See e.g. Marko Milanovic, "Extraterritorial Derogations from Human Rights Treaties in Armed Conflict," in *The Frontiers of Human Rights: Extraterritoriality and its Challenges*, ed. Nehal Bhuta. Oxford: Oxford University Press, 2016; Stuart Wallace, "Derogations from the European Convention on Human Rights: The Case for Reform," *Human Rights Law Review* 20 (2020): 769.

References

Al-Skeini and Others v. the United Kingdom [GC], no. 55721/07, 7 July 2011

Amann v. Switzerland [GC], no. 27798/95, 16 February 2000

Arai, Yutaka "The Margin of Appreciation Doctrine in the Jurisprudence of Article 8 of the European Convention on Human Rights," *Netherlands Quarterly of Human Rights* 16 (1998)

Banković and Others v. Belgium and Others (decision) [GC], no. 52207/99, 12 December 2001

Big Brother Watch and Others v. the United Kingdom [GC], nos. 58170/13 and 2 others, 25 May 2021

Boothby, William H. "Biometrics" in *New Technologies and the Law in War and Peace*, ed. William H. Boothby. Cambridge University Press, 2019.

Buhrow, William, *Biometrics in Support of Military Operations: Lessons from the Battlefield* (Boca Raton: CRC Press, 2017)

Bykov v. Russia [GC], no. 4378/02, 10 March 2009

Carter v. Russia, no. 20914/07, 21 September 2021

Case concerning the Temple of Preah Vihear (Cambodia v. Thailand) (judgement) [1962] ICJ Rep 260, 15 June 1962

Catt v. the United Kingdom, no. 43514/15, 24 January 2019

Cymutta, Sebastian, "Biometric Data Processing by the German Armed Forces during Deployment," NATO CCDCOE Research Paper (2021)

Delval, Eugénie "The Kunduz Airstrike before the European Court of Human Rights: a glimmer of hope to expand the Convention to UN Military Operations, or a tailored jurisdictional link?" *The Military Law and the Law of War Review* 59 (2021)

de Vries, Karin "Right to Respect for Private and Family Life," In: *Theory and Practice of the European Convention on Human Rights*, eds. Pieter van Dijk, Fried van Hoof, Arjen van Rijn and Leo Zwaak. Cambridge, Antwerp, Portland: Intersentia, 2018.

Fernández Martínez v. Spain, no. 56030/07, 15 May 2012

Geiß, Robin and Henning Lahmann, "Protection of data in armed conflict" *International Law Studies* 97 (2021)

Georgia v. Russia (II) [GC], no. 38263/08, 21 January 2021

Harris, David, Michael O'Boyle, Ed Bates and Carla Buckley, *Law of the European Convention on Human Rights.* Oxford: Oxford University Press, 2018.

Issa and Others v. Turkey, no. 31821/96, 16 November 2004

ISO/IEC International Standard 2382-37, "Information Technology – Vocabulary – part 37: biometrics 2" (2012)

Jain, Anil, Arun Ross, Salil Prabhakar, "An introduction into biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology* 14 (2004)

Jehova's Witnesses of Moscow v. Russia, no. 302/02, 10 June 2010

Karabeyoğlu v. Turkey, no. 30083/10, 7 June 2016

Keegan v. Ireland, Series A no. 290, 26 May 1994

Khelili v. Switzerland, no. 16188/07, 18 October 2011

Klass and Others v. Germany, Series A no. 28, 6 September 1978

Klaus Müller v. Germany, no. 24173/18, 19 November 2020

Kokott, Juliane and Christoph Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law* 3 (2013)

Koorndijk, Jeanice "De Verwerking van Biometrische Gegevens tijdens Stability-policing-operaties van de Nederlandse Krijgsmacht: Richting Lessons Learned ter Verbetering van het Juridisch Kader" (Master's thesis, University of Amsterdam, 2021)

Leander v. Sweden, Series A no. 116, 26 March 1987

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Rep 883, 9 July 2004

Linskov Jacobsen, Katja "Biometric data flows and unintended consequences of counterterrorism," *International Review of the Red Cross* 103 (2021)

Liu, Nancy Y. *Bio-privacy: Privacy Regulations and the Challenge of Biometrics.* Milton Park, Abingdon, Oxon; New York: Routledge, 2012.

Lubin, Asaf "The Rights to Privacy and Data Protection under International Humanitarian Law and Human Rights Law," forthcoming in *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, eds. Robert Kolb, Gloria Gaggioli and Pavle. Kilibarda. Cheltenham: Edward Elgar Publishing, 2022.

Lunan, Mark, "New Doctrinal Concepts: Biometrics," *The Three Swords Magazine* 33 (2018)

Medvedyev and Others v. France, no. 3394/03, 10 July 2008

Milanovic, Marko, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy.* Oxford: Oxford University Press, 2011.

Milanovic, Marko "Al-Skeini and Al-Jedda in Strasbourg," *European Journal of International Law* 23 (2012)

Milanovic, Marko "Extraterritorial Derogations from Human Rights Treaties in Armed Conflict," in *The Frontiers of Human Rights: Extraterritoriality and its Challenges*, ed. Nehal Bhuta. Oxford: Oxford University Press, 2016.

Milanovic, Marko "European Court Finds Russia Assassinated Alexander Litvinenko," EJIL:Talk!, September 23, 2021. https://www.ejiltalk.org/european-court-finds-russia-assassinated-alexander-litvinenko/.

Mitchell, Alison "Distinguishing friend from foe: law and policy in the age of battlefield biometrics notes and comments," *Canadian Yearbook of International Law* 50 (2012)

M.K. v. France, no. 19522/09, 18 April 2013

M.N. and Others v. Belgium (decision) [GC], no. 3599/18, 5 May 2020

M.N. and Others v. San Marino, no. 28005/12, 7 July 2015

P. and S. v. Poland, no. 57375/08, 30 October 2012

Piechowicz v. Poland, no. 20071/07, 17 April 2012

Rodica Mihaela Rotaru v. Romania, no. 34325/05, 10 November 2009

Roman Zakharov v. Russia [GC], no. 47143/06, 4 December 2015

S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, 4 December 2008.

Sandu and Others v. the Republic of Moldova and Russia, nos. 21034/05 and 7 others, 17 July 2018

Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, 27 June 2017

Schabas, William. *The European Convention on Human Rights: A Commentary.* Oxford: Oxford University Press, 2015.

Szabó and Vissy v. Hungary, no. 37138/14, 12 January 2016

Talbot, Rohan "Automating occupation: International Humanitarian and Human Rights Law implications of the deployment of facial recognition technologies in the Occupied Palestinian Territory" *International Review of the Red Cross* 102 (2020)

Tan, Floris and Marten Zwanenburg, "One step forward, two steps back? Georgia v Russia (II), European Court of Human Rights, Appl No 38263/08," *Melbourne Journal of International Law* 22 (2021)

Vavřička and Others v. the Czech Republic [GC], nos. 47621/13 and 5 others, 8 April 2021

Vig v. Hungary, no. 59648/13, 14 January 2021

Wallace, Stuart "Derogations from the European Convention on Human Rights: the case for reform," *Human Rights Law Review* 20 (2020):

Zwanenburg, Marten "Know thy enemy: the use of biometrics in military operations and International Humanitarian Law" *International Law Studies* 97 (2021)