Presentation for the 23rd Congress of the International Socierty of Military Law and the Law of War

Protection of personal data in military operations, including peace operations

Marten Zwanenburg

1 Introduction

Ladies and gentlemen, dear colleagues,

It is a truism that information plays an increasingly important role in military operations. This information is often in digital form, and is then referred to as data. Some of this data may be so-called personal data. There is not one uniform definition of personal data in international law. However, the General Data Protection Regulation of the European Union, commonly referred to as the GDPR, provides an authoritative definition. This directive states in Article 4 (1) that personal data means:

> any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The adoption of the GDPR in 2016 underlined the importance that member States of the EU attach to the protection of personal data. But it is not only EU member states which consider personal data protection to be important. Protection of such data is considered an important issue across the globe. This is illustrated by the fact that several resolutions of the UN General Assembly have stressed the need for personal data protection. On particularly important resolution in this regard is UNGA resolution 45/95 adopted already in 1995.

Personal data protection is considered important because it safeguards personal integrity, promotes trust in digital interactions, and upholds the fundamental rights of individuals in an

increasingly data-driven world. This statement links such protection to the human right to privacy, a point to which I will return later.

Because of the importance attached to personal data, many if not all states have domestic legislation protecting such data. Personal data is also protected under international law, in at least two ways. First, personal data is part of a person's privacy. As such it is covered by the right to privacy in international human rights instruments. Second, there are international instruments that specifically deal with the protection of personal data. Two of these deserve particular mention. The first is the EU GDPR which I have already mentioned. The second is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108. In 2018 a protocol amending the convention was adopted, modernising the convention. This modernised version of the convention is referred to as convention 108+ and is expected to enter into force in the near future.

What all this means for the protection of data during military operations has only started to receive attention relatively recently. This concerns questions such as: "Do military operations have to protect the personal data of persons they come into contact with?"; "If so, what does this require of them?"; and "Does the military personnel taking part in such an operation have the right to have their personal data protected?".

In this presentation, I will discuss the question of protection of personal data in military operations. I will start by focusing on the two legal frameworks I mentioned before, the right to privacy and data protection law. I will then discuss whether and how the situation is different during an armed conflict. I will conclude by saying a few words about protection of personal data in peace operations.

In the time available for this presentation, it is impossible to deal with this topic in any detail. I will therefore focus on setting out some key issues and open questions.

2 The right to privacy

The right to privacy is set out in a number of human rights instruments, including Article 17 of the ICCPR and Article 8 of the ECHR. It may be noted that different treaties use different

terms. Whereas the ICCPR refers to "privacy", the ECHR uses the expression "private life". These terms are however understood to refer to the same right.

Although the right to privacy is thus firmly entrenched in human rights treaties, there is no agreement on the exact scope and content of the right. What is clear is that there are different aspects, or types, of privacy that each are part of the right to privacy. There is by now general agreement that so-called "informational privacy" is one of those aspects of the right to privacy. Informational privacy has been described as "typified by the interest in preventing information about one-self to be collected and in controlling information about one-self that others have legitimate access to."

One open question regarding the right to privacy concerns to what extent armed forces operating outside their own territory are bound by the human rights obligations of their state. In other words, does the right to privacy also apply extraterritorially? The starting point in answering that question is that the ICCPR and the ECHR provide that a state must provide human rights protection to persons "within their jurisdiction". There is broad support for the view that a state exercises jurisdiction extraterritorially in two cases. The first is when it exercises effective control over an area. The second is when it exercises authority and control over an individual throught its agents. A typical example of the latter is when a person is detained in the context of a military operation.
There is also a view that a person falls within the jurisdiction of a state when conduct of that state has direct and reasonably foreseeable effect on human rights. This view, which has been adopted by the UN Human Rights Committee, looks at control over the exercise of rights, rather than control over territory or an individual. This approach is however contested, and was rejected by the ECtHR a few months ago in its admissibility decision in the case of Augusto Duarte and others v. Portugal and others.

Another way to approach this is to look at where the personal data is processed. The ECtHR has held in its recent judgment in the case of Wieder and Guarnieri v UK that is it important where effects are produced by the act in question rather than the place where the alleged victim is present for the purposes of determining whether jurisdiction is exercised.

With regard to a state's own military personnel, there is debate whether they fall within the jurisdiction of the sending state in the sense in which that term is used in human rights. The

admissibility decision by the ECtHR in the case of Toledo Polo v. Spain of in 2022 suggests that this is not the case, but a British court in the case of Smith (no. 2) did accept this.

In cases where the right to privacy does apply extraterritorially, there are various open questions concerning the application of that right in the context of a military operation. One of these concerns the legal basis for the interference with privacy. The right to privacy is not absolute: it may be interfered with if several conditions have been met. One of these conditions is that there must be a basis in law for the interference. Can a United Nations Security Council (UNSC) resolution form such a legal basis? The case law of human rights monitoring bodies on the right to privacy only refers to domestic legislation, but it does not exclude the possibility that a UNSC resolution can constitute a legal basis. That case law however also suggests that the resolution will have to meet certain substantive conditions. Specifically, it needs to be publicly accessible, clear, precise, comprehensive, and non-discriminatory.

3 Data protection

As mentioned above, the two main international instruments concerning protection of personal data are the EU's GDPR and Convention 108+.

The GDPR according to Article 2 does not apply to activities which fall outside the scope of EU law, such as activities concerning national security. It also does not apply when carrying out activities in relation to the common foreign and security policy of the EU. This effectively means the GDPR does not apply to military operations. However, certain states, such as the Netherlands, have adopted domestic legislation expanding its application to military operations unilaterally.

Convention 108 provided for the possibility to exclude from the scope of application of the convention certain categories of automated personal data files. Convention 108+ however no longer makes this possible. In principle therefore, it applies to military operations, including outside of EU member states. This follows from the Convention's scope of application set out in Article 1. That article provides that the Convention protects every individual, whatever his or her nationality or residence, with regard to the processing of their personal data.

Article 11 of the updated convention does provide for certain exceptions from a number of the convention's provisions when this constitutes a necessary and proportionate measure in a democratic society for the protection of, among others, national security and defense. Further exceptions are allowed with reference to processing activities for national security and defense purposes. But these exceptions are subject to strict limits. For example, they must be provided by law. They are also subject to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective party.

It follows that even where the exceptions to Convention 108+ can be invoked, certain basic principles of data protection apply to military operations under that convention. States carrying out such operations will need to determine whether their domestic legal framework meets the requirements of the Convention.

Protection of personal data is not just important for the local population in the area of operation of a military operation. It is also important for the personnel carrying out that operation. This may require specific measures. As an illustration, US President Biden issued an Executive Order Presidential Directive in February of this year which aims to prevent the large-scale transfer of Americans' personal data to countries of concern and provides safeguards around other activities that can give those countries access to Americans' sensitive data. The press release accompanying this order refers expliclty to the military service members.

4 Protection during armed conflict

An important question is whether the applicable legal framework for protection of personal data changes when there is an an armed conflict making international humanitarian law (IHL) applicable.

As a starting point, IHL itself does not contain rules that explicitly addres the protection of personal data. Such protection can however be read into certain rules of IHL. One example is the protection of medical data. Under IHL, medical services and infrastructure enjoy specific protection. Civilian hospitals for example must "at all times be respected and protected by the Parties to the conflict." It has been argued that based on the broad and unqualified scope of

such protection, such protection includes medical data. This would include patient records for example.

In addition to IHL, human rights law and Convention 108+ will continue to apply. There is nowadays broad support for the view that human rights, including the right to privacy, continue to apply during armed conflict in principle. Human rights treaties provide for the possibility to derogate from the right to privacy, for example in article 4 of the ICCPR. Such derogation is however subject to strict limitations. The same applies to the exceptions provided for in Article 11 of Convention 108+.

5 Protection in peace operations

In peace operations, personnel of troop contributing states come to the operation with their own legal framework for personal data protection. This may lead to issues of interoperability, because those frameworks will not always be the same. For example, some sending states may be bound by Convention 108+ and others not.

In the case of peace operations led by international organizations, there is broad support for the view that the organizations themselves also have relevant obligations. For example, the UN accepts that it is bound by human rights. The main argument for this appears to be that based on its international legal personality, it is bound by customary international human rights. This however raises the question of the exact scope of the right to privacy under customary international law. For example, it is has been questioned whether the right extends to online privacy.

If the operation is led by an international organization, that organization could put in place a policy that mitigates such issues. This does not appear to be the case at present, however. To the best of my knowledge, the UN for example does not have an overarching policy on data protection for UN peace operations. The 2023 updated UN policy on the protection of civilians in UN peacekeeping does state that "confidentiality must be respected for any information that could be used to identify sources." This is however the only sentence in that document that refers to protection of personal data. The 2011 Policy on human rights in UN peace operations only refers to protection of personal data in the context of activities by the human rights component of a peace operation.

In 2018, the UN High Level Committee on Management (HLCM) formally adopted 'Principles on Personal Data Protection and Privacy'. These principles set out a basic framework for the processing of "personal data" by, or on behalf of, the United Nations System Organizations in carrying out their mandated activities. The principles are however not binding, and it is unclear if they are applied in the context of peace operations.

In principle, peace operations are bound by the domestic law of the host state in which they operate. This domestic law may include provisions on protection of personal data. However, these provisions will in most cases not be enforcable in relation to the peace operation because of the immunity from jurisdiction that the operation enjoys under a Status of Forces Agreement or similar agreement.

6 Conclusion

Ladies and gentlemen, this brings me to a number of final remarks. In this presentation, I have attempted to provide an overview of the protection of personal data in military operations. Because of the limited time available, this overview has been very broad-brush. Nevertheless, it is possible to conclude that military operations are not a legal vacuum when it comes to the protection of personal data.

The right to privacy in international human rights law provides for such protection, a protection that does not cease entirely even when this right is derogated from. For states parties to Convention 108+, this instrument also provides certain limits to interference with personal data. Finally, in the context of an armed conflict certain rules of IHL can be interpreted as providing a measure of protection for personal data.

The application of these legal frameworks to the protection of personal data also raises many questions however. This presentation has highlighted some of them. Going forward, it will be important to address these questions.

Many states are doing so at the domestic level. It is logical that states do this because they all have their own unique legal system and political sensitivities to take into account. At the same time, I think it would be very useful for states to exchange views on these questions and to share

best practices. This could avoid duplication of work and contribute to interoperability between armed forces. The International Socierty for Military Law and the Law of War in my view could play a useful role in this context, for example by distributing a questionnaire on this topic leading up to its next Congress, as has been done in the past on other topics.

Thank you for your attention.

***