Data Protection in Armed Conflict

Robin Geiß 2021-02-15T12:11:49

These days, our thoroughly digitalised societies run on data. Indeed, the notion of data is embedded in the very concept of digitalisation, and no process or service that relies on computing power is conceivable without it. It is therefore only natural that experts of international humanitarian law (IHL) have for a while now pondered over the question of how to treat data under the existing legal frameworks applicable to armed conflicts, starting from the premise that, in the words of the International Committee of the Red Cross, military operations affecting data "could cause more harm to civilians than the destruction of physical objects". At the same time, the debate has at times suffered from ambiguities and inaccuracies concerning the subject matter.

Military cyber operations can affect civilian data in different ways, depending on the means of conduct and the operation's target. For example, a ransomware operation against a hospital might lead to the encryption of critical patient data, forcing the hospital to postpone important surgeries or even shut down entirely. Since the beginning of the Covid-19 pandemic, malicious cyber activity against healthcare facilities has surged, as could be witnessed at a Düsseldorf hospital last September where the hospital was forced to de-register from providing emergency care. Further damaging scenarios involving data are easily conceivable. Server breaches at private companies might put large amounts of sensitive business data into the hands of the adversary, enabling it to exploit it for blackmailing or extortion – the company itself as well as individual employees, potentially disclosing intimate personal details. Leaking financially relevant data could lead to the crashing of stock markets and vast economic damage in the target states.

The ongoing discussion concerning the status and possible protection of civilian data in armed conflict is in need of increased clarity and granularity. There are two aspects in particular that might advance the deliberations. First, one might ask whether there are certain types of civilian data that merit specific legal protection due to their critical properties. Second, development of the law should focus on a possible regulation of what states are permitted to do with civilian data obtained during armed conflict.

Terminology and Distinctions

Data can be categorized as "content-level data" or "operational-level data", with only the former category representing information intelligible to humans. While some scholars consider such data as outside the scope of IHL, it is what most experts implicitly refer to when talking about the protection of "data" during armed conflict. A further, normative distinction of different types of data on the content level is between personal and non-personal data. Scholars of IHL exploring the protection of data in armed conflict usually deal not with "data protection" – analysing how personal

data may be processed by persons or entities that control the data – but with “data security”, which concerns the confidentiality, integrity, and availability of the IT systems that process the data and thus of the data itself.

The Protection of Data Under IHL

Adversarial cyber operations that target “operational-level data” should not be analysed as being directed against data at all. This is because from a technical perspective, nearly every conceivable type of cyber operation targets “data” even though the “object of attack” is the system that runs on the data. For instance, the “Crash Override” malware used to take down the power grid in Kiev in December of 2016 did take effect by altering operational data that ran the grid’s control systems. Therefore, in order to assess what rules of existing IHL might apply and whether the operation would be prohibited due to a violation of the principle of distinction (Article 48(1) Additional Protocol I (AP I)), the principle of proportionality (Article 51(5)(b) AP I), or of the duty of precautions in attack (Article 57 AP I), one needs to look at the consequences of the operation.

For this reason, the question of “data protection” proper during armed conflict should zoom in on cyber operations that target content-level data. Certain civilian infrastructures enjoy specific protection under IHL, including, most importantly, medical services and infrastructures, which “must be respected and protected by the parties to the conflict at all times”. There is general agreement, including among states, that this protection comprises personal medical data, for example patient records or other information relating to individuals in treatment. Moreover, as cyber operations that target objects indispensable for the survival of the civilian population are prohibited, data necessary for the functioning of these especially protected objects and services is protected as well.

These explicitly regulated cases aside, however, the protection of content-level data in armed conflict has remained an unsettled and contentious issue. For one, it is unclear how to subsume data under the existing terminology of IHL. Whereas Article 52(2) AP I formulates the fundamental principle of distinction by stipulating that “[a]ttacks shall be limited strictly to military objectives”, these are defined as “objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage”. As targets lacking an object-quality therefore do not fall within the scope of the principle of distinction, data is only protected by IHL if it can be considered an object in this sense.

The debate surrounding this question comes down to two main positions. Proponents of the first view contend that the notion of “object”, taking its ordinary meaning, implies that the target of the military operation must be an entity of a physical quality, that is visible and tangible in the real world, which data quite obviously is not. When a cyber operation targets data, IHL only becomes relevant if this leads to physical effects on a physical object. The opposing position holds that data can indeed be considered an “object” following a teleological interpretation

which reveals that in light of the overarching purpose of Additional Protocol I to improve the protection of victims of armed conflict, an overly restrictive and literal understanding of “data” would result in a protection gap of IHL. As noted by Kubo Ma#ák, “many targets whose physical equivalents are firmly protected by IHL from enemy combat action would be considered fair game as long as the effects of the attack remain confined to cyberspace” if data is lacking object-quality.

The Inherent Limitations of Existing IHL

The ongoing debate among experts and policymakers has revealed the inherent limitations of existing IHL, which at its core is concerned with the *physical effects* of armed conflict. As a consequence, existing protections at most encompass cyber operations against the availability or the integrity of data, but *only* if they entail physical or otherwise tangible harmful consequences. Operations against the confidentiality of data, for example in the context of surveillance or espionage, but also for the purpose of misusing personal data in order to coerce or otherwise influence the behaviour of individuals in situations of armed conflict, are outside the scope of existing IHL unless they fall into a specially protected category of data.

Given the significance of data for modern digitalised societies, we propose a paradigm shift: To date, the prevalent debate has taken the rules and principles of existing IHL and applied them to “data”. A novel approach would be to take, as a starting point, the principles of existing data protection, data security, and other pertinent legal frameworks and attempt to apply them to contemporary armed conflict. Such an approach might be better suited to accommodate the actual relevance of data for the information society and to address the protection needs during armed conflict.

In reversing the direction of consideration, the leading question then becomes: *Should* certain types and uses of data enjoy protection from adversarial cyber operations in armed conflict, *irrespective of* whether data qualifies as an “object” or not, and even if they do not cause harmful (physical) consequences?

Securing the confidentiality of personal data – one of the core principles of existing data protection frameworks like the GDPR – is mostly outside the scope of what has so far been considered to require or deserve protection during armed conflict. However, the harm to individual civilians could nevertheless be significant, even absent physical effects. As repeatedly confirmed by domestic courts around the world, the right to privacy is derived from and serves as a protection of the dignity of a person. A complete collapse of privacy of the civilian population during armed conflict as a consequence of adversarial military cyber operations would be a paradigm shift of how wars are fought and could conceivably lead to a paralysis of the targeted civilian society at large.

Advancing the Debate

As a starting point, the possible protection of the confidentiality of (personal) civilian data could approach the question in relation to two distinct aspects. First, one might focus on the properties of the data itself and ask whether there are certain types of civilian data that should enjoy increased protection in and of themselves. For example, the GDPR acknowledges “special categories of personal data” that are, “by their nature, particularly sensitive in relation to fundamental rights and freedoms” and thus “merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms” (Recital 51 GDPR). These properties include “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership” as well as “genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation” (Art. 9(1) GDPR). None of these “special categories of data” lose any of their sensitivity during armed conflict.

Second, the discussion should zoom in on a possible regulation of what adversarial states that obtain civilian data through military cyber operations during armed conflict are permitted to do with that data. For example, while it is inconceivable to establish a prohibition of surveillance and espionage activities during armed conflict, one might contemplate a rule against certain specified uses of the collected data, such as publishing or leaking sensitive personal data and/or a rule against exploiting such data sets for the purpose of coercion, extortion, or manipulation.

The current debate surrounding the extent of “data protection” in situations of armed conflict must move beyond the exclusive focus on the object-quality of data. The different ways data – and the attached rights and interests of individuals and societies that data incorporates – can be affected by cyber operations require us to contemplate what kind of approach will be necessary to grasp and adequately protect the various functions of data in our digitalised societies.
