Complementary, but imperfect.

Some currently available legal mechanisms for protecting individual privacy in the course of military activities

Ann Väljataga

Law Researcher

ann.valjataga@ccdcoe.org

CCDCOE

Structure

1. Weapons reviews
2. GDPR data protection impact assessments
3. EU dual-use regulation

Weapons reviews

CCDCOE

Weapons reviews

- → An IHL provision that regulates (also) peacetime activities
- → Based on Art. 36 GC API, national policies and/or customary international law
- → Requires reviewing new weapons, means or methods of warfare against any applicable rule of international law (including IHRL)

Applicability

- → A strict reading suggests that only normal expected employment scenarios should be reviewed, not data collection for decision support purposes
- → However, in an integrated system technically it may be hard to pinpoint when data collection and analysis ends and employment begins
- → Therefore if data-driven decision support is integrated with the harming mechanism of a capability, data collection practices should also be reviewed against applicable international law (including IHRL)

Limitations and challenges

- → Only as strong as the protection provided by an applicable human rights treaty (questions over applicability remain)
- → Weak accountability, complex individual enforceability; only brings about liability if primary IHL/IHRL rules breached
- → First and foremost a preventive measure of mitigating legal risks
- → Limited scope, according to a narrow interpretations only technologies that are designed to cause disrupitve effects are reviewed
- → Questionable independence and expertise of the review committees
- → Typically a one-off procedure

Strengths

- → Anchored in IHL legality (non-derogable in conflict)
- → State-level accountability (cannot be outsourced to industry)
- → Covers military-specific contexts
- → Prevents unlawful weapons entering service

GDPR Data protection impact assessments

CCDCOE

GDPR DPIA

- Under Article 35 of the GDPR, a DPIA must be conducted when data processing is likely to result in a high risk to the rights and freedoms of natural persons—for example:
  - Use of biometric identification or facial recognition technologies
  - Deployment of automated decision-making systems, especially in surveillance or targeting
  - Monitoring of individuals in public or semi-public areas (e.g. border control using AI-based tools)
  - Large-scale processing of sensitive data such as health or criminal records of staff or civilians

Applicability

- → Applies also to private defence contractors operating in the civilian market or dual-use contexts (e.g. AI tools for both civilian and military use)
- → No blanket exemption for all defence-related processing.
- → A solid protective measure against the privacy violations that might take place while developing dual-use capabilities by private defence contractors

Limitations and challenges

- → Limited territorial scope of applicability
- → Does not apply to purely military operations or intelligence activities carried out by national defence forces if the activity is convincingly framed as a matter of national security
- → Does not easily enforceable meaningful remedies for individuals, due to postponement of notification
- → Questionable independence of in-house DPOs

Strengths

- → Failure to conduct or properly perform a DPIA can result in serious administrative fines (up to €10 million or 2% of turnover), which is a meaningful deterrent for private contractors.
- → DPIA framework requires assessing risks not just to data protection but to all fundamental rights and freedoms under the EU Charter
- → DPIAs reach into the supply chain and private industry, where weapons reviews might not

EU Dual-use Regulation 2021/821

CCDCOE

EU Dual-use Regulation

- Regulation (EU) 2021/821 (Dual-Use Regulation), which entered into force in September 2021. It modernised the previous framework by:
  - Extending controls to cyber surveillance technologies (e.g. biometric tools, hacking software).
  - Requiring exporters to assess human rights risks, not just proliferation risks.
  - Introducing a “catch-all” clause allowing member states to restrict exports of non-listed items when there is a risk of internal repression or serious human rights violations.

Applicability

- → Exporting states and licensing authorities; companies must comply with license requirements
- → Cross-border transfers of dual-use goods, software, and technologies (civil/military or surveillance)
- → Pre-export: before technology, software, or systems leave the jurisdiction

CCDCOE

Limitations and challenges

→ Scope gaps: not all privacy-invasive tech covered

→ Focuses on exports, not domestic development or use

→ End-use monitoring difficult once exported

Strengths

- → Directly addresses cross-border proliferation of surveillance/dual-use tech
- → Applies to both industry and state exporters
- → Creates leverage over global markets (blocking exports to repressive regimes)
- → Explicit human rights clause

Summary - a patchwork of protection.

+ Covering different actors

→ The three instruments span the civilian–military and peacetime–wartime divides

→ When combined, the three offer protection within a relatively broad territorial scope

→ The three cover efficiently the *ex ante* phases of R&D, testing, procurement and export

-Prevention-heavy orientation

- → **Weapons Reviews**: in practice, they can become *one-off box-ticking exercise*. Limited information about states actually revisiting reviews once a system is deployed or upgraded.
- → **DPIAs**: By design, *ex ante* risk assessments; strongest before processing begins, weaker once systems are operational.
- → **Export Controls**: Work only at the point of export licensing. Once a system crosses borders, oversight stops; monitoring actual use is minimal.

Other legal mechanisms to consider

→ National and EU defence procurement regulations

→ EU and national AI legislation

→ Soft law, ethics and due diligence frameworks

→ …

Thank you!

CCDCOE