Privacy International's statement for Informal Exchanges on Artificial Intelligence in the Military Domain, Session 11 - Existing and Emerging Normative Proposals

[CHECK AGAINST DELIVERY]

17 June 2026

Chair, Excellencies, ladies and gentlemen

PI would like to make four observations regarding existing and emerging proposals.

Firstly, international human rights law provides a legally binding framework applicable throughout the entire lifecycle of AI. HRL is applicable in peace and war time, including to the development, deployment and use of AI in the military domain.

Secondly, it is imperative that states initiate a global process toward a binding international instrument that bans and strictly regulates autonomous weapons systems (AWS).

The treaty should:

- ban autonomous weapons that do not allow for meaningful human control;
- ban autonomous weapons that target humans directly;
- provide additional rules so that other autonomous weapons will be used with meaningful human control;
- recognise privacy and data protection as core human rights obligations integral to any meaningful regulatory framework. It must address the entire lifecycle of these technologies, from research and development to deployment, export, and oversight.

Thirdly, the human rights implication of AI systems in military domain beyond AWS needs to be addressed.

States should reject the use of 'defence' or 'national security' as a blanket justification to bypass regulation, and instead demonstrate legality, necessity, proportionality, and independent oversight in all AI systems in military domain.

They should:

- ensure that ongoing international efforts to regulate AI in the military domain explicitly articulate states' obligations to respect and protect privacy and personal data;
- adopt a moratorium on the use of AI systems for the use of force, for example in decision support systems, until necessary international rules and effective safeguards are in place;
- provide transparency on the use of AI and other data-driven technologies in the military domain, including the measures taken to mitigate human rights risks; and
- adopt privacy and data protection legislation, in line with international standards, that protects privacy and personal data in the military domain, setting out clearly what categories of personal data may be processed, on what legal basis, subject to what safeguards, and with what oversight.

Lastly the role of companies must be addressed. The UN Guiding Principles on Business and Human Rights provide the reference framework.

Under this framework, companies should:

- stop developing, selling, transferring or servicing autonomous weapon systems that operate without meaningful human control, and stop supplying AI systems for the use of force, until necessary international rules and effective safeguards are in place;
- carry out effective human rights due diligence to identify, prevent and mitigate the risks of adverse human rights impacts arising from their activities in the military domain;
- demonstrate compliance with international data protection standards, including by adopting data protection policies, clearly setting out what categories of personal data may be processed in military domain context, on what legal basis, subject to what safeguards, and with what oversight; and
- ensure that licences, deployment terms and acceptable-use policies for AI models used by military or government customers include binding minimum data-protection obligations, including in relation to personal data about civilians and other affected third parties.

Thank you Chair.