

Committee: Disarmament and International Security Committee (DISEC)

Topic: Privacy Risk of AI

Sponsors: Algeria, Brazil, Chile, China, Somalia, Pakistan, the United States of America, Russian Federation

Signatories: Germany, Italy, the Republic of Korea, the United Kingdom, France, Australia, Canada

The General Assembly,

Recognizing the increasing global reliance on artificial intelligence technologies and the privacy risks associated with data collection, processing, and dissemination,

Emphasizing the need for international cooperation that respects national sovereignty, technological diversity, and the varying levels of development among member states,

Highlighting the importance of developing flexible and non-binding international norms that promote responsible artificial intelligence development while protecting the rights and dignity of all nations,

1. Encourages Member States to adopt Ethical Impact Assessment (EIA) Mechanism in respective jurisdiction, by which the transference, collection, analysis, and any utilization of private information in any manifestations over quantity of which defined thereby, with due respect to sovereign decisions of Member States, through which the authorities may understand the impact thereof and assess the benefits with the potential risk, and in that regards:
 - a. Calls on the UNESCO, with the purposes and principles enshrined in UNESCO Recommendation of AI Ethics (2001), to establish a sub-committee on digital privacy protection, reporting on a yearly basis thereto on its work progress, which is entitled and obliged to
 - i. Assist Member States in their development of governance technology and integration of artificial intelligence in governance;
 - ii. also assist Member States in the promulgation and codification of sovereign-led data protection regulations that are referenced of the assessment and suggestions by the subcommittee
 - b. Reaffirms that technical standards should prioritize:
 - i. Public safety and resilience against AI misuse;
 - ii. Protection of sensitive personal data and critical national infrastructures;
 - iii. Promotion of innovation, especially in emerging economies, by avoiding undue technical barriers to entry;
 - c. Emphasizes that participation in technical standard exchanges must remain voluntary, non-binding, and respect the principle of national sovereignty in AI governance and technological development.

- d. Encourages Member States to enact provisions in national codes with regard to sensitive personal information, defined by respective national regulations, to ensure that the utilization thereof in any and all manifestations is conducted via explicit consent of the users;
- 2. Confirms the global consensus that all activities concerning the collection and the usage of data should be conducted in a lawful, necessary, and proportionate manner that fully respects the rule of law, international human-rights obligations, and democratic values, thereby safeguarding individual privacy and bolstering public trust in AI-enabled technologies, and confirms the need to enhance transparency concerning
 - a. the methods employed by public- and private-sector actors to collect data for AI systems,
 - b. the types and sensitivity levels of personal or non-personal data gathered, and
 - c. the specific purposes and modalities of subsequent processing or re-use;
- 3. Encourages AI developers to voluntarily disclose, in publicly accessible reports, under the guidance of national authorities, for the purpose of enhancing transparency, fostering trust, and reducing the risks associated with misuse:
 - a. The general sources of training data, in order to enhance transparency and foster trust among stakeholders, utilized in the development of AI models, including but not limited to:
 - i. Public databases;
 - ii. Licensed datasets;
 - iii. Open-source resources and other legally obtained materials;
 - b. The intended sectors and fields for the deployment of AI technologies, to ensure the responsible and context-appropriate use of AI systems, including but not limited to:
 - i. Healthcare,
 - ii. Education,
 - iii. Commerce and other relevant industries;
- 4. Invites Member States to:
 - a. Submit national case studies detailing their experiences in regulating and protecting privacy within AI applications, particularly including:
 - i. Challenges encountered;
 - ii. Solutions adopted;
 - iii. Measurable outcomes achieved, to serve as references for future discussions on building internationally recognized standards for AI governance;
 - b. Share lessons learned, to collectively contribute to the formulation of future international frameworks, focusing on:
 - i. Regulation of personal data processing;
 - ii. Mitigation of privacy risks;

- iii. Balancing innovation with the protection of fundamental rights;
 - iv. Promoting mutual learning among Member States;
 - v. Assisting developing countries in building capacity for data governance and privacy protection;
 - vi. Encouraging the formation of regionally tailored yet globally connected frameworks;
- 5. Further suggests that the sharing of case studies be coordinated through platforms such as UNESCO, the International Telecommunication Union (ITU), or other relevant UN agencies;
- 6. Reaffirms the principles that participation in transparency mechanisms and sharing of case studies should remain voluntary, non-binding, and fully respectful of each Member State's sovereignty and unique legal and socio-economic context;
- 7. Establishes International Dialogue Platforms, wherein countries can fund or support international NGOs, such as the International Crisis Group or associations like the Peace and Technology Alliance, to bring together experts, scholars, military advisors, and tech industry representatives from different nations.
 - a. These platforms aim to discuss the regulation and ethics of AI weapons development
 - b. These platforms also aim to promote the creation of cross-national codes of conduct to prevent the misuse of AI technology in warfare;
- 8. Recognizes the important role Non-Governmental Organizations (NGOs) plays in international and national AI privacy protection and development efforts and encourages countries can to or support international NGOs, such as the International Crisis Group or associations like the Peace and Technology Alliance, to bring together experts, scholars, military advisors, and tech industry representatives from different nations, aiming to discuss the regulation and ethics of AI weapons development and promote the creation of cross-national codes of conduct to prevent the misuse of AI technology in warfare;
- 9. Takes notes of the efforts made by NGOs that monitor the military application of AI and beyond, such as the Campaign to Stop Killer Robots, and encourage countries can encourage civil society to propose regulatory measures and issue risk warnings, ensuring greater transparency in policymaking and pressures governments and corporations to comply with human rights standards and international law when deploying AI in military contexts;
- 10. Decides to establish the International AI and Conflict Resolution Forum, a permanent global forum where policymakers, AI researchers, ethicists, and military leaders regularly meet to discuss how to prevent AI from escalating conflicts, with the long

term goal of drafting guidelines, sharing best practices, and working towards treaties that regulate the use of AI in military applications and beyond, in which:

- a. An annual summit gathering experts in AI, international law, peace studies, and defense technology would be established, which would serve as a platform to review AI developments, assess emerging risks in warfare, and propose collaborative projects aimed at using AI for peacekeeping and humanitarian missions, and in that regard:
 - i. Form a special office as a subsidiary body under the General Assembly that focuses exclusively on monitoring the use of AI in warfare,
 - ii. The offices would have the mandate to investigate abuses, mediate disputes involving AI-driven conflicts, and propose suggestions for the General Assembly nations or groups that may inflict disputes on international AI ethics agreements;
 - b. The final goal of the summit is to reach consensus on an international AI privacy and security accord that specifically addresses the protection of personal data and privacy in the context of AI used during conflicts:
 - i. This accord would recommend strict limitations on the collection, use, and sharing of data by AI systems in military and surveillance operations and beyond,
 - ii. This accord also requires independent audits to ensure transparency and examines nations or organizations that misuse AI to violate individual rights during times of war and beyond;
11. Decides to establish the Global Ethical AI Certification Program for Defense Technologies, which is an international certification program where AI systems intended for military use must pass rigorous ethical and privacy standards before deployment, which would involve collaboration between governments, human rights organizations, and AI experts. Systems would be assessed for their compliance with international humanitarian law, respect for civilian privacy, and ability to avoid unlawful surveillance or targeting;
12. Calls upon specialized agencies, funds, programmes, other entities, bodies and offices, and related organizations of the United Nations system, within their respective mandates and resources, to continue to assess and enhance their response to leverage the opportunities and address the challenges posed by artificial intelligence systems in a collaborative, coordinated and inclusive manner, through appropriate inter-agency mechanisms, including by conducting research, mapping and analysis that benefit all parties on the potential impacts and applications; reporting on progress and challenges in addressing issues; and cooperating with and assisting developing countries in capacity building, access and sharing the benefits of safe, secure and trustworthy artificial intelligence systems in achieving all Sustainable Development Goals and sustainable development in its three dimensions - economic, social and environmental; stressing the need to close artificial intelligence and other digital divides between and within countries;

13. Affirms that the protection of personal data should respect national sovereignty, recognizing that each State has the right to establish its own regulatory frameworks in accordance with its cultural, political, and developmental contexts, and further emphasizes that the design and implementation of privacy laws must allow flexibility for countries at different stages of digital development, taking into account the need to:
 - a. Foster innovation and technological advancement without imposing undue compliance burdens;
 - b. Ensure that privacy protections are adaptable to the specific economic capacities and institutional realities of each nation,
 - c. Support the right of all Member States, particularly developing countries, to pursue digital transformation policies that balance privacy, growth, and societal well-being,
 - d. Avoid the imposition of rigid, one-size-fits-all international standards that undermine national priorities and sustainable development goals,
 - e. Calls for the adoption of the BAGEL Framework — Balanced Approaches for Governance, Ethics, and Localization — aimed at safeguarding national autonomy in privacy protection by
 - i. Encouraging flexible legal structures that prioritize both privacy and innovation,
 - ii. Promoting culturally contextualized privacy standards that respect unique national identities;
14. Taking notes on the importance of promoting AI development in countries with limited hardware resources in order to improve the livelihood of citizens through the development of life-changing AI technology;
15. Recommends the betterment of local regional relationships by the establishment of peace deals in exchange for technological resources;
16. Encourages Member States to create AI-powered tools to aid, promote, and empower institutions fighting for human rights and social equality, in which that:
 - a. Special importance will be given to areas with socio-economic difficulties.
 - b. Employment of AI to aid in the education of the younger generations in the usefulness and dangers of AI tools;
17. Determines to bridge the artificial intelligence and other digital gap between the developing and developed countries;
18. Calls upon Member States to cooperate, taking action on information exchange and education support.