Documentation of the Simulation of the

Human Rights Council (HRC)*

Conference B

13 - 17 April 2025

* National Model United Nations (nmun.org) organizes simulations of the United Nations. The resolutions in this document were the work of dedicated college and university students attending our conference. They are not official United Nations documents, and their contents are not the actual work of the United Nations entity simulated.

Human Rights Council (HRC)

Committee Staff

Director	Theodore Alberto
Assistant Director	Evan Sun
Chair	Jack Stuart

Agenda

1. The Right to Privacy in the Digital Age
2. Safeguarding Human Rights in Peaceful Protests and Assemblies

Resolutions adopted by the Committee

Code	Topic	Vote (In favor - Against - Abstention)
HRC/1/1	The Right to Privacy in the Digital Age	Adopted without a vote
HRC/1/2	The Right to Privacy in the Digital Age	Adopted without a vote
HRC/1/3	The Right to Privacy in the Digital Age	Adopted without a vote
HRC/2/1	Safeguarding Human Rights in Peaceful Protests and Assemblies	Adopted without a vote
HRC/2/2	Safeguarding Human Rights in Peaceful Protests and Assemblies	Adopted without a vote

Summary Report

The Human Rights Council held its annual session to consider the following agenda items:

1. The Right to Privacy in the Digital Age
2. Safeguarding Human Rights in Peaceful Protests and Assemblies

The session was attended by representatives of 33 Member States.

On Sunday, the committee adopted its initial agenda, beginning discussion on the topic of “The Right to Privacy in the Digital Age.” By Tuesday, the Dais had received a total of three proposals covering a wide range of subtopics, including personal cybersecurity education, combating cybercrime, regulating artificial intelligence, increasing protection measures for personal data, and limiting the widespread collection of personal data. Delegates began diplomatic discussion on how to ensure the right to privacy can be adopted at an international level.

On Wednesday, 3 draft resolutions were approved by the Dais, one of which had an amendment. The committee adopted all 3 resolutions without a vote. The resolutions represented a wide range of issues, including ethical guidelines, data security standards, infrastructure, and transparency measures. Furthermore, on Wednesday, the committee began to collaborate on the topic of “Safeguarding Human Rights in Peaceful Protests and Assemblies.” By the end of the final session, 3 draft resolutions had been approved by the Dias, none of which had amendments, yet only 2 draft resolutions were adopted without a vote.

Code: HRC/1/1
Committee: Human Rights Council
Topic: The Right to Privacy in the Digital Age

The Human Rights Council,

Guided by the purposes and principles of the *Charter of the United Nations* (1945),

Emphasizing Article 12 under the *Universal Declaration of Human Rights* (UDHR) (1948), which declares that all individuals have the right to privacy, including protection from arbitrary interference,

Recognizing Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) (1966), which reaffirms privacy as a human right and affirms that personal data protection is inherent to that right to privacy,

Further guided by the General Assembly's resolution 79/1 on “The Pact for the Future” and its annex, the “Global Digital Compact,” in establishing ethical guidelines for the protection of privacy and freedom of expression for all,

Highlighting its resolution 51/17, which emphasizes the challenges of maintaining the right to privacy in the digital age,

Recalling its resolutions 28/16 and 54/21, which emphasize that the same rights individuals have offline must also be protected online,

Further emphasizing its resolution 54/21, which outlines the important role of Member States in having access to citizens’ digital data in order to protect national security,

Bearing in mind the General Assembly resolution 78/265 calling for the implementation of trustworthy systems for the sustainable development of new technology, considering the ever-evolving nature of technology and digitalization,

Deeply concerned that in 2022 alone, there were 3,225 recorded cyberattacks, which resulted in 343 million victims worldwide, as stated in the 9662nd Security Council meeting,

Acknowledging the United Nations *Guiding Principles on Business and Human Rights* in preventing human rights impacts as a guideline for Member States to protect, address, and remedy violations,

Mindful of each Member State’s sovereignty in constructing national guidelines that align with their respective cultural and political values,

Acknowledging objective 5.1 of the Cape Town Global Action Plan for Sustainable Development Data on strengthening partnerships between national and international entities for the development of statistical systems with all public and private sectors, such as private corporations and the banking sector, involved in the production and use of data for sustainable development,

Deeply regretting that over 64% of online applications were sharing data with third-party users, raising concerns about online privacy and consent, according to its resolution 25/1,

Noting with zest that General Assembly resolution 68/167, which calls for all Member States to respect the right to privacy and to take measures to put an end to the violations of all rights to digital privacy, was the first resolution that explicitly addressed the rights to digital privacy and legitimized the concerns of many Member States,

Alarmed that among the least developed countries, only 45% of nations safeguard citizens' rights to data privacy and protection, according to the United Nations Trade and Development's (UNCTAD) *Data and Privacy Unprotected in One-Third of Countries, Despite Progress* report (2020),

Affirming General Assembly resolution 79/125 on the importance of digital literacy to ensure the right to privacy,

Further recognizing the value of the United Nations Development Programme (UNDP) in providing knowledge sharing and education initiatives on digital privacy, such as the Digital Security Open Online Course developed by the Caribbean Digital 4 Development Hub,

Acknowledging the International Telecommunication Union's (ITU) Digital Skills Toolkit, a comprehensive guide for governments to develop responsible digital strategies to be implemented nationally to ensure individuals have the needed skills to be more employable, productive, and successful in the digital scope,

Emphasizing further a need for improved preparedness for digital transformation, and to help enable governments to evaluate their data and resources,

Recalling Security Council resolution 2748 from Member States within African regions, which discusses the importance of using a holistic approach to inform citizens of beneficial information that can protect less developed countries from potential forms of digital interference,

Further alarmed that as many as 97% of users globally do not read the terms and conditions before accepting them, which poses a potential threat to users' digital privacy, according to the Deloitte survey *You're Not Alone, No One Reads Terms of Service Agreements* (2017),

Further acknowledging the 1992 General Assembly report, further working to discuss the details of new forms of technologies and their potential impacts, considering less developed countries and their specific needs for digital privacy,

Expressing its conviction against the misuse of digital platforms to spread misinformation or dangerous information that may harm the individual or the state,

Having considered that companies mainly focused on digital marketing and social media have access to sensitive information like personal communications, and that such information sharing needs to be regulated, according to the Office of the High Commissioner for Human Rights (OHCHR) *Content Regulation in The Digital Age* (2018),

Commends UNDP's *Data Privacy, Ethics, And Protection Guidance Note On Big Data For Achievement Of The 2030 Agenda,* which is a guide that helps regulate and ensure government access to citizens' data, ensuring such access is grounded in strict legal and ethical standards and transparently monitored,

Acknowledging the different developmental capacities of developed and developing Member States in their design and implementation of data protection frameworks, and the challenges that the developmental divide creates in the ability to protect citizens' private data,

Highlighting that there is no global standard or international law for Member States to follow as a framework for ensuring the right to digital privacy,

Noting with concern its resolution 51/17 that focused on recent trends concerning the right to privacy, such as the abuse of intrusive hacking tools and the risk of creating systems with pervasive surveillance and control,

Considering the United Nations Office of Disarmament Affairs (UNODA) definition on national security, which describes it as the ability of a State to support its citizens with protection and defense,

Recognizing the value of the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) Global Network Initiative in working alongside Member States to protect the data security of global citizens,

Appreciating the work of the UNDP's Digital Readiness Assessments, which allows Member States to understand their technological developmental contexts,

Further recalling UNESCO's *Recommendation on the Ethics of Artificial Intelligence,* which provides global standards for the ethical use of Artificial Intelligence (AI) with human rights and dignity as the bedrock,

1. *Requests* Member States to utilize the ITU's *Digital Skills Toolkit*, overseen by the Economic and Social Council (ECOSOC), which offers a guide for Member States to create effective national digital skills strategies and policies to enhance the digital literacy of individuals, an important skill in ensuring privacy in the digital age;

2. *Recommends* the ITU, under direction from ECOSOC, to implement ethical guidelines into its *Digital Skills Toolkit* for both private and public sectors in the use and the extraction of sensitive data, noting that:

    a. Governments should have access to their citizens' data when considered necessary to safeguard national security as defined by the UN, such as in instances of emergency, security breaches, or immediate harm or threat to the well-being of citizens, or the security of the nation, and such data should be kept for a limited amount of time at the discretion of the individual Member State;

    b. Private technological companies should clearly request access to consumer data and plainly express the specific use of the data to the consumer;

    c. Financial institutions should seek permission from consumers before engaging in third-party data sharing, with relevant actions that pose a threat to national security being alerted to the Member State governments;

    d. The healthcare sector should be free to determine what information shall be liable for dissemination amongst healthcare institutions, with government regulations prioritizing the protection and security of each patient's data;

3. *Directs attention* to the importance of Member States' promotion of digital literacy to their citizens, recognizing vulnerable populations such as children, low-income, or senior citizens as a priority, and considering the disparities in Member States' technological development, through national and non-governmental programs such as:

    a. Communication actions towards including public awareness campaigns through traditional media (radio, television, and journalism) and digital platforms (official government websites and verified social media accounts);

    b. Inclusion of digital literacy into the national educational curricula;

    c. Communication channels between the government, citizens, and the private sector to provide individuals with accessible and clear information on how personal data is used by public and private actors;

    d. Non-governmental organizations (NGOs) and think-tank workshops to educate citizens and the government on the current issues of data privacy, such as the *Electronic Protection Information Center*, which works to provide research and bolster education on digital privacy through events, panels, and seminars;

4. *Encourages* all Member States to utilize the *Digital Readiness Assessment* proposed by the UNDP as a framework to evaluate and strengthen national policies on data protection, cybersecurity, and digital privacy, with a focus on safeguarding personal information in public and private digital platforms;

5. *Urges* the OHCHR to collaborate with the UNDP in expanding existing digital literacy and privacy education, such as the Digital Security Open Online Course developed by the Caribbean Digital 4 Development Hub, to other hubs especially in less developed regions by providing digital literacy materials that align with regional standards for educational and labor institutions to ensure that all individuals are aware of their national and regional digital privacy protections;

6. *Invites* Member States to model national digital programs after UNESCO's *Global Network Initiative,* which works to protect the freedom of digital privacy by encouraging private sector companies to develop and follow principles for responsible online digital conduct based on existing guidelines that respect the privacy of users;

7. *Calls upon* the Special Rapporteur on the Right to Privacy to prepare a supplementary report to the *UN Guiding Principles on Business and Human Rights*, on the role of digital technology and AI in business, to be aligned with the UDHR;

8. *Further suggests* Member States develop and implement national policies, reviewed by OHCHR, that promote transparency and user comprehension in the terms and conditions provided by private companies, to ensure meaningful and informed consent by users, by:

    a. Requiring that all legally binding clauses within terms and conditions be clearly highlighted, bolded, or otherwise made visually distinct, to draw the user's attention to their significance;

    b. Ensuring that terms and conditions are written in clear, concise, and plain language, easily understandable by the average user regardless of legal or technical background;

    c. Promoting the use of summaries or layered formats that allow users to quickly grasp the key points of the terms, with the option to access full legal text for further details;

    d. Encouraging regular reviews and updates to company terms and conditions to maintain clarity and relevance, and to reflect changes in law or business practices;

9. *Advocates* for ECOSOC to proclaim financial data as sensitive information internationally and take note of the need for succinct, tailored national legislation over electronic transactions and fiscal processes to set ethical standards for transparency between domestic government and private companies;

10. *Further calls upon* Member States to determine what type of data can be harvested from citizens and what information isn't shareable, ensuring that:

    a. Information shared must require a consensus between the State and the individual;

    b. Member States have the final say in the information that is to be shared between all parties;

11. *Further urges* Member States to review existing digital security frameworks to ensure total compliance with international human rights, as set out in the Universal Declaration of Human Rights, including the right to privacy;

12. *Requests* the expansion of the UNDP's regional courses such as the Digital Security Massive Open Online Course to be tailored between regions as reflective of regional legal frameworks, such as the ASEAN Human Rights Declaration and the African Union on Human and People's Rights, in ensuring that

individuals understand specific digital privacy rights afforded to them under international, regional, and domestic legislation;

13. *Further recommends* Member States to model National AI policies after UNESCO's *Recommendation on the Ethics of AI*, which has been used in countries to implement digital technology regulation policies that are focused on the ethical development and use of AI systems;

14. *Advocates* for Member States to adopt a domestic cybersecurity infrastructure to safeguard public order and social stability through the prevention of the spread of misinformation, cybercrime, and data breaches in order to prevent external technological infringement of individuals' digital records and data;

15. *Promotes* the continuous assessment by the Special Rapporteur of how Member States' national regulations are addressing technological innovations due to the impact of expanding digitalization and the risks of data becoming vulnerable to the potential misuse by malicious outside actors;

16. *Encourages* Member States to utilize the United Nations Statistical Division's *UN Guide on Privacy-Enhancing Technologies for Official Statistics*, which works to promote the use of technologies that safeguard users' digital privacy by providing a framework for and encouraging countries to adopt privacy-preserving techniques such as encryption and data anonymization to protect the right to digital privacy;

17. *Invites* the United Nations Technology Bank to collaborate with Member States of the Global South to pursue collaborative technological advancement while safeguarding digital rights to privacy, promoting both innovation and the sovereign protection of personal data;

18. *Recommends* the Special Rapporteur on the Right to Privacy to issue a report identifying best practices and resource-effective strategies for developing Member States to protect the security of civilians' data, aligning with international human rights law, accounting for diverse political and economic capabilities, drawing on relevant regional frameworks such as the ASEAN Data Management Framework and the Malabo convention;

19. *Further recommends* the implementation of an International Digital Rights and Privacy Declaration (IDRPD) under UNDP, modeled after the EU's Declaration on Digital Rights and Principles, which will aim to:

    a. Encourage the creation of international standards supporting data transparency and collection, as well as use limitation, conscious of regional, cultural, and economic disparities based on the Special Rapporteur's Right to Privacy Report;

    b. Provide technical assistance to Member States, especially developing Member States, in drafting and implementing a data protection legislation framework aligned with international standards, including support for institutional capacity building of data protection authorities;

    c. Support public education campaigns on digital privacy and cybersecurity, and;

    d. Encourage equitable access to privacy-enhancing technologies (PETs);

20. *Encourages* multilateral collaboration amongst Member States in constructing national legal frameworks with acknowledgment of Human Rights Council resolution 54/21, focusing on privacy protection matters in the digital era to prevent conflict with the national interests between Member States.

Code: HRC/1/2
Committee: Human Rights Council
Topic: The Right to Privacy in the Digital Age

The Human Rights Council,

Gravely concerned that in 2023, an estimated 8.2 billion records were breached globally, according to the United Nations Office of Counterterrorism (UNOCT) Report Beneath the Surface (2024),

Acknowledging Article 12 of the *Universal Declaration of Human Rights* (1948), which states that all individuals are entitled to privacy and protection against unlawful interference,

Reaffirming the principles of the General Data Protection Program (GDPR), such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and accountability, which are based on the protection of data subjects, ensuring that their data is collected, processed, stored, and erased in licit and transparent ways,

Emphasizing General Assembly resolution 78/265, regarding the existence of varying levels of technology development between Member States, considering capabilities and financial assistance, the enhancement of digital literacy within less developed countries, and a necessity for achieving SDG 10 on reduced inequalities,

Observing the work of the World Economic Forum Digital Trust initiative and studies conducted by the Center for Strategic and International Studies (CSIS), which promote global standards for data security, privacy, and ethical digital practices,

Noting with concern the growing number of cybersecurity attacks conducted by terrorist actors, as expressed by the United Nations Office of Counterterrorism,

Calling attention to Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) (1966), and General Assembly resolution 79/175, which reiterates privacy as a human right and strives to protect citizens from invasive technologies used maliciously by the private sector,

Observing the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which is a voluntary framework developed by NIST to manage and reduce cybersecurity risks,

Bearing in mind the Universal Periodic Review (UPR), a peer-review process of the Human Rights Council (HRC) that records every 4.5 years, acts as a catalyst to implement national laws for a safer digital space,

Considering the *2030 Agenda for Sustainable Development*, adopted by all United Nations Member States in 2015, which created 17 Sustainable Development Goals (SDGs) aiming for "peace and prosperity for people and the planet" while tackling climate change and working to preserve oceans and forests,

Recalling the findings of the United Nations E-Government Survey, which highlights the importance of digital governance in enhancing public service delivery, promoting citizen engagement, and advancing transparency, accountability, and sustainable development through the strategic use of information and communication technologies (ICTs),

Recognizing the Cyber4Good initiative by the International Telecommunication Union (ITU), which emphasizes the use of digital innovation to address global humanitarian challenges, including health, education, and food

security, by fostering inclusive access to technology and promoting digital solutions that support the achievement of the SDGs,

Reiterating the importance of collaborative mechanisms to oversee the use of personal data to promote corporate accountability, under SDG 17 (partnerships for the goals),

Aware of the United Nations Human Settlements Programme (UN-Habitat), which emphasizes the opportunity for growth in the global digital infrastructure, especially for developing countries,

Calling attention to the United Nations Educational, Scientific, and Cultural Organization's (UNESCO) inputs for the preparation of the thematic report of the Office of the United Nations High Commissioner for Human Rights (OHCHR), in which it is iterated that balancing the right to privacy with other fundamental rights in the digital age requires clear legal principles and a proportionality-based approach to data protection,

Viewing with appreciation the Global Counter-Terrorism Program on Cybersecurity and New Technologies (GCT), which focuses on helping Member States and international organizations develop and implement effective strategies to counter terrorism, particularly in digital space,

Noting its resolution 54/21 and General Assembly resolution 75/176, which emphasize the importance of the right to privacy in the digital age and urge Member States to ensure the protection of personal data, especially sensitive health-related information, in the context of digital communication and technological advancements;

Taking into account the World Health Organization (WHO) *Global Strategy on Digital Health 2020–2025*, which promotes the use of digital technologies to enhance health systems, expand access to care, and ensure that digital health solutions are implemented in accordance with principles of human rights, data protection, and ethical responsibility,

Deeply concerned that over 18,000 human rights violations were recorded by the Human Rights Case Database (HRCD) in 2023, with a 62% follow-up rate by national institutions and human rights courts,

Underscoring the International Telecommunications Union (ITU) annual AI for Good Global summit as the leading multilateral conference for AI development and digital improvement, with the assistance of global technological companies and research institutions,

Appreciating regional policies such as the ASEAN Data Management Framework and the AI Governance and Ethics Guide in setting out priorities, initiatives, and principles for data privacy,

Acknowledging the positive impact of frameworks such as the United Arab Emirates' Federal Decree No. 45 on personal data protection in ensuring the protection of citizens' data, promoting international data privacy, and addressing corporate data exploitation,

Taking note of its resolution 56/45, which encourages improved coordination through multilateral dialogue,

Taking into account the dangers that arise with the collection of individuals' data from mass surveillance conducted by public and private companies, with the costs of data breaches rising from $3.86 million to $4.24 million in 2021, according to the IBM Cost of a Data Breach Report 2021 in collaboration with the Ponemon Institute,

1. *Highlights* the importance of Member States acknowledging that the protection of personal data is closely linked to the right to privacy and is based on a series of commonly recognized principles, related to data protection and privacy, in line with the spirit of General Assembly resolution 79/175, such as:

a. Purpose limitation: data must be collected and used only for specific purposes and clearly communicated to the data subject;

b. Minimization: only data strictly necessary to achieve the stated purpose must be collected;

c. Transparency: individuals must be informed about how their data is collected, used, and processed;

d. Quality and accuracy: data must be precise and up to date;

e. Access: individuals must be able to access their data and request its modification or deletion;

f. Security: data must be protected by appropriate technical and organizational measures;

g. Accountability: data collection should include accessible mechanisms for individuals to report concerns, complaints, or violations of their privacy;

2. *Invites* the OHCHR to partner with the ITU in creating a digital privacy side-event at the annual AI for Good Global Summit in order to:

    a. Foster international dialogue on ethical surveillance, best practices for data protection, and emerging digital policies, drawing from similar systems such as the OHCHR HRCD;

    b. Include further participation of universities, research centers, non-governmental organizations (NGOs), and independent bodies, to keep up to date with emerging technologies, such as non-invasive mechanisms;

    c. Consider regional standards such as the Association of Southeast Asian Nations (ASEAN) AI Governance and Ethics Guide, in adapting approaches to different national contexts;

3. *Fully supports* Member States to collaborate with each other in promoting the *Voluntary Integration of Rights* (1948), General Assembly resolution 79/175 on the “Right to Privacy in the Digital Age” (2024), and principles developed by HRC, into national legal frameworks related to digital privacy and data protection;

4. *Welcomes* Member States to incorporate such norms into domestic legal frameworks through inclusive legislative processes, ensuring adaptability to national contexts while maintaining core principles of human rights protection;

5. *Suggests* collaboration among Member States to harmonize digital privacy standards where feasible, aiming to reduce disparities in enforcement and to foster mutual recognition of data protection frameworks, especially where cross-border data flows are involved;

6. *Draws attention* to principles on data security, drawing upon existing regional frameworks such as the ASEAN Data Management Framework;

7. *Considers* the creation of a voluntary International Framework on Surveillance Ethics, to be discussed under its leadership with support from relevant UN bodies such as OHCHR, the Special Rapporteur on the Right to Privacy, and the ITU, with the goal of guiding Member States in the ethical use of surveillance technologies by securing digital privacy, in alignment with current United Nations initiatives such as its resolution 54/21 and General Assembly resolution 79/175 on the right to privacy in the digital age;

8. *Further invites* Member States create national legal policies based on pre-existing frameworks, like the General Data Protection Regulation and ASEAN Data Management Framework, in monitoring violations

such as unauthorized access, and commercialization of personal data, with the help of strict regulations, which emphasize the specific terms and regulations emphasised by the United Nations officially, that users must agree to and specify what information that is collected, specifically targeted to the private sector;

9. *Requests* Member States to model initiatives after the World Economic Forum Digital Trust initiative, which promotes global standards for data security, privacy, and ethical digital practices, along with focusing on the dimension of cybersecurity, transparency, and fairness through collaboration between governments, businesses, and civil society;

10. *Recommends* that Member States model national policies after the UN-Habitat *People Centered Smart Cities* program, which facilitates transparent data governance, and strong cybersecurity measures for least developed countries by prioritizing the development of privacy protection and accessibility through the:

    a. Collaboration with diverse stakeholders to build smart city projects, infrastructure, and services to enhance access to privacy;

    b. Expansion of the capacity of city staff for digital transformation;

    c. Evaluation of the need for technology and addressing equality, environmental sustainability, and inclusion in smart city initiatives;

11. *Calls upon* Member States to develop sovereign initiatives, after ITU's Cyber4Good initiative, which promotes ethical digital privacy rights through bridging the cybersecurity gap in least developed countries with the objectives of increasing incident response capabilities, support in national cybersecurity strategies and governance, and skills development by providing tools, training, and expertise from the global partners;

12. *Further calls upon* Member States to consider the GCT as a means of enhancing national capabilities to develop and protect critical infrastructure against cyber attacks by terrorist organizations, emphasizing that robust cybersecurity measures prevent attacks, and also safeguard the individual right to privacy, achieved by offering guidance on ethical surveillance, and conducting capacity-building workshop for law enforcement;

13. *Calls for* Member States to foster collaboration between private multinational corporations and public entities over the use and sharing of personal data by:

    a. Encouraging Member States to facilitate public and private partnerships (PPP) under their jurisdiction, considering principles from frameworks such as the United Arab Emirates' Federal Decree No. 45 on personal data protection, and international agreements by Member States;

    b. Facilitating the development of frameworks to improve collaboration between the public and private sectors in managing cyber risk, considering the implementation by Member States of an international framework modeled after the NIST Cybersecurity Framework (CSF);

14. *Suggests* Member States promote the development of inclusive and secure digital health systems, including the implementation of telemedicine services and the digitalization of patient health records, with the aim of expanding access to healthcare in remote and underserved areas, while ensuring the protection of personal health data, in line with General Assembly resolution 75/176 and the WHO *Global Strategy on Digital Health 2020–2025*;

15. *Encourages* Member States to recognize concerns of data privacy invasions raised by the CSIS regarding the excessive collection of sensitive personal data by governments through private digital companies, including information related to health, finances, religion, familial status, and geolocation, and address these concerns by:

    a. Utilizing encrypted digital platforms to ensure continuity of care and safeguard medical data from unauthorized access;

    b. Supporting capacity-building programs for healthcare professionals and administrators to manage digital health systems effectively and ethically, in accordance with international standards on data protection and privacy;

16. *Encourages* Member States to form online national databases similar to the United Nations E-Government Knowledge base, focusing on the protection of personal data use, accessible by all citizens to ensure transparency, and governmental institutions that can:

    a. Ensure the availability of data relating to the right to privacy in digital spaces while guaranteeing the protection of sensitive and personal information;

    b. Guarantee the accessibility of online publications on the utilization of personal data by corporations;

    c. Recommend funding opportunities for individuals interested in doing research to improve digital spaces;

17. *Directs attention* of Member States in utilizing the UPR to include in their submissions, assessing national digital privacy legislation, in relation to international human rights standards and its effectiveness in protecting the right to privacy of all individuals, including through safeguards against the misuse of surveillance technology, unlawful data protection, and discriminatory digital practices;

18. *Encourages* Member States to develop a national and international strategies to enhance cybersecurity awareness and digital resilience, in close collaboration with the United Nations Office of Cybersecurity and New Technologies (OCNT), particularly in light of increasing global internet access, by:

    a. Distributing accessible and user-friendly materials on key topics such as phishing prevention, safe browsing habits, data protection, and secure password practices;

    b. Organizing annual “Cybersecurity Week” events in schools and communities to promote public engagement, build grassroots awareness, and cultivate a culture of cybersecurity and AI literacy;

    c. Integrating digital literacy and cybersecurity into national curricula at all levels of schooling, ensuring long-term digital resilience and awareness amongst future generations.

Code: HRC/1/3
Committee: Human Rights Council
Topic: The Right to Privacy in the Digital Age

The Human Rights Council,

Acknowledging Article 12 of the *Universal Declaration of Human Rights* (1948) that emphasizes the protection of every individual's privacy,

Reaffirming its 54/21 (2023) that asserts the protection of privacy is essential for the realization of other fundamental rights,

Recalling the General Assembly resolution A/78/L.49 (2024) on the development of safe and trustworthy AI systems,

Acknowledging the Universal Periodic Review (UPR) developed in General Assembly resolution 60/251 as the leading mechanism for holding Member States accountable for their human rights obligations,

Recognizing its resolution 54/21, which emphasizes the importance of continuous and regular reassessments of national digital technology legislation and practices to ensure alignment with international human rights law and emerging technologies,

Reaffirming its report hat notes the use of non-inclusive datasets for AI systems is discriminatory and violates fundamental human rights, particularly towards vulnerable populations,

Emphasizing the Office of the High Commissioner for Human Rights (OHCHR) report (A/HRC/48/31), which ensures the right to be informed about the collection and use of personal data, the right to object to data processing, and the right to restrict processing under certain conditions,

Acknowledging the United Nations Terminology Database (UNTERM) is a multilingual terminology database maintained jointly by the main duty stations and regional commissions of the United Nations system,

Appreciating the work of the International Telecommunications Union (ITU) in facilitating global connectivity, such as through the GIGA Initiative, which provides internet access to schools in Member States that may be classified as Least Developed Countries (LDCs),

Acknowledging the Internet Governance Forum (IGF) and its importance as a platform for international cooperation on internet safety and protocols,

Noting with appreciation the positive effects on data privacy of the General Data Protection Regulation (GDPR) implemented in the European Union, ensuring fair and lawful processing of data, purpose limitation, data minimisation, and data retention,

Noting with approval the utilization of app-based electronic governance systems, collaborating with financial institutions that ensure the security, protection, and universal access of public and private services,

Acknowledging the necessity of balancing national security interests with the protection of individual rights in cyberspace,

Fully aware of the increasing malicious use of artificial intelligence (AI) technologies and AI-powered surveillance systems around the world, as evidenced by the University of Cambridge's report "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation",

Recognizing the key objectives of the Global Digital Compact (GDC), specifically Objective 4, which includes advancing more responsible interoperable governance and ensuring the right to be informed about the collection and use of personal data, the right to object to data processing, and the right to restrict processing under certain conditions,

Believing that digital literacy, which involves the confident and critical use of a full range of digital technologies for information, communication, and basic problem-solving in all aspects of life, as is defined by UNESCO, is a fundamental set of competencies, necessary for individuals to adequately and safely utilise digital technologies,

Recognizing that digital literacy is a growing part of any approach to skills development, as it features in the International Children's Fund's (UNICEF) framework, which seeks to prepare children and adolescents for school, work, and life,

1. *Encourages* Member States to adopt or update national legislation concerning both private and public development of AI systems to ensure all such systems developed or deployed within their jurisdiction are developed with unbiased and non-discriminatory programming, aligned with international law on anti-discrimination, and ensuring that:

    a. AI systems under development are informed by internationally recognized inclusive and disaggregated data sets that reflect diverse lived realities of population groups, including women, children, those with disabilities, indigenous communities, and other marginalised groups;

    b. Systems are assessed by national experts qualified by Member States for discriminatory practices, such as racial and gender discrimination, before being released to the public;

    c. Bias audits are conducted by national experts to routinely assess for biases throughout the AI software's development timeline, ensuring appropriateness and a non-discriminatory nature;

2. *Suggests* Member States strengthen their national laws on data privacy, following the example of preexisting legislation such as the European Union's General Data Protection Regulation, through:

    a. Inclusion of principles such as informed consent, guaranteeing sufficient understanding by all parties of how data will be transformed into meaningful information; data minimization, allowing data controllers to retain only personal information that is directly relevant and necessary to accomplish a specified purpose and user rights to data access and erasure, allowing individuals to retrieve their personal data as soon as it is no longer necessary in relation to the purpose for which it was collected or processed;

    b. Developing national accountability mechanisms for data privacy breaches by private companies operating within the Member State, such as investigations, audits, or sanctions;

    c. Recognising the need for region-specific legislation, influenced by the history, cultural background, political landscape, and level of digitalisation of the Member State in question;

3. *Recommends* that Member States adopt, at the national level, a transparent, trustworthy, privacy-preserving, and human-centric approach to both public and private development of artificial intelligence, as reminded in the General Assembly resolution A/78/L.49 (2024), through:

a. Underlining the importance of the principle of AI explainability, which, if implemented, ensures that AI systems' algorithms and output are traceable and understandable for humans;

b. Promoting robust human oversight of AI systems' development;

c. Reminding the importance of continuous research on the matter of AI systems' impact on data privacy and surveillance;

4. *Advocates* that the General Assembly Third Committee expand the objectives of the IGF, and extend its duration for another 10 years until 2036, and to provide a knowledge sharing platform for less developed Member States, by establishing a capacity building session for less developed Member States to share knowledge on developing and expanding domestic legislation on data protection and privacy laws;

5. *Establishes* the appointment of a new working group under HRC, to be named "The Working Group on AI and Surveillance Justice" (WGAISJ), made up of experts on technology and human rights, tasked with producing annual reports on the intersections between mass surveillance and the use of AI tools to profile people;

6. *Calls for* the appointment of a new Special Rapporteur on the Ethical Use of Artificial Intelligence in Surveillance to monitor, assess, and provide guidelines on the use of AI technologies for surveillance purposes by:

    a. Conducting assessments of AI-driven human rights violations, such as data privacy breach committed by both state and non--state actors due to AI-powered surveillance systems collecting personal data from social media, phones, or CCTV footage without individuals' knowledge, through a framework that consists of reviews of national legislation and policies and on site visits to Member States that consent to an evaluation;

    b. Providing recommendations to Member States on the best course of action for ethical AI use, as defined by United Nations Department of General Assembly and Conference Management (DGACM) through the UNTERM database, a linguistic tool that provides access to a diverse multilingual terminology, as the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings;

7. *Suggests* the International Telecommunication Union (ITU) to prioritize digital literacy and protections within their frameworks and existing initiatives by:

    a. Expanding the existing GIGA initiative to include digital privacy training as a fourth pillar;

    b. Promoting the inclusion of digital privacy in the ITU's *Connect 2030 Agenda* plans;

8. *Encourages* the OHCHR to develop training materials for the expansion of the ITU GIGA initiative, led by local facilitators, to ensure all students with new digital access have effective digital privacy legislation;

9. *Encourages* the National Educational Systems of all Member States to promote school courses to help young people have a better understanding of general Internet security and give them the tools to manage privacy issues by:

    a. Supporting teachers with specified tutors to help them with the new technologies;

    b. Promoting programs such as ICDL (International Certification of Digital Literacy) a global social enterprise committed to raising standards of digital competence in the workforce, education and society which is currently available in more than 100 countries, and DQ Every Child which is a

global movement to empower young people with comprehensive digital citizenship skills from the start of their digital lives;

10. *Invites* Member States to launch campaigns on digital privacy that aim to:

    a. Raise awareness on the importance of safeguarding personal data and privacy in the digital environment through targeted, multilingual campaigns adapted to different demographics, including youth, the elderly, and vulnerable communities;

    b. Educate individuals on actionable steps to protect their digital rights, such as enabling two-factor authentication, managing privacy settings, recognizing phishing attempts, and understanding terms of service;

    c. Collaborate with educational institutions, civil society organizations, and technology companies to integrate digital privacy modules into school curricula and lifelong learning programs;

11. *Further requests* Member States to provide workers with resources such as digital training programs and framework to implement practical digital safety measures, covering topics such as:

    a. Fundamentals of information and application security and the Security Incident Management;

    b. Safety in industrial applications;

    c. Open source Intelligence (OSINT) that will strengthen corporate immunity to potential cyber-attacks or data threats;

    d. Technical standards provided by organizations like ministries and national institutes that companies must follow to protect data and ensure cybersecurity, as a set of practices, technologies, and processes to prevent misuse, disclosure, and abuse of systems;

12. *Encourages* Member States to implement national legislation for private enterprises engaging in digital data gathering to ensure that all citizens' rights to privacy are protected in alignment with international frameworks such as the OHCHR report on the right to privacy (A/HRC/48/31);

13. *Recommends* that governments and institutions adopt legislation establishing the explicit right of individuals to give, withdraw, and manage their consent regarding the use of their personal data, drawing on frameworks such as the OHCHR resolution 54/L.12/Rev.1, and further encourages the integration of mechanisms that ensure individuals have clear, accessible, and enforceable control over how their data is collected, stored, and used, including legal protections for both privacy and intellectual property;

14. *Urges* Member States to include within their Universal Periodic Reviews, assessments of their national digital privacy legislation, evaluating its alignment with international human rights standards and its effectiveness in safeguarding human rights, such as the right to privacy;

15. *Expresses appreciation* for the collaboration between financial institutions that offer their regulated software services, and the government, to further strengthen the security and privacy of national social services used by the private sector, to provide equality in privacy protections through the use of a singular software system, provided and funded by the government and accessible for everyone, by consolidating all social services into one app;

16. *Welcomes* the public and private sectors to engage in open dialogue regarding digital privacy, with the goal of overseeing the access and functions of the app to support users.

Code: HRC/2/1
Committee: Human Rights Council
Topic: Safeguarding Human Rights in Peaceful Protests and Assemblies

---

The Human Rights Council,

Taking into consideration articles 19 and 20 of the *Universal Declaration of Human Rights* (UDHR) (1948), which state that all individuals have the right to freedom of expression and the right to freedom of peaceful assembly and association without interference,

Acknowledging article 21 of the *International Covenant on Civil and Political Rights* (ICCPR) (1966), which reaffirms freedom of speech as a fundamental right and guarantees the realization of those rights of those who participate in a peaceful assembly, consequently affirming its importance in democratic practices,

Calling attention to articles 10 and 11 of the *European Convention on Human Rights* (1950), which reiterate the right to freedom of expression and to freedom of assembly and association, stating that no restrictions shall be placed upon protesters, unless national security or public safety is compromised,

Keeping in mind article 2 of the Code of Conduct for Law Enforcement Officials, which stipulates that authorities shall respect, maintain, and uphold human rights,

Emphasizing its resolution 25/38 on the role of the government in facilitating rather than obstructing peaceful assemblies, while ensuring public safety,

Recalling its resolution 38/11 on the promotion and protection of human rights during peaceful assembly, which underlines the important role of communication between organizers, protesters, local authorities, and officials exercising law enforcement duties in the proper management of peaceful assemblies,

Reaffirming the General Assembly report 72/178 made by the Special Rapporteur of Torture that states the prohibition of torture and other cruel, inhuman or degrading treatment or punishment in circumstances where extra-custodial use of force by State agents occur,

Recognizing the vital role of civil society organizations, independent media, and human rights defenders in upholding and promoting the right to peaceful assembly,

Reminding the principles of legality, necessity, proportionality, accountability, and non-discrimination as the basis of police action presented in the General Assembly resolution 34/169 on “Code of Conduct for Law Enforcement Officials”,

Keeping in mind the European Law Enforcement Directive (LED), which regulates how police forces should use citizens’ data for security purposes to ensure that activists can use social media freely to organize protests,

Recognizing the de-escalation techniques and non-violent crowd control are recommended by the Office of the High Commissioner for Human Rights (OHCHR) in *Less Lethal Weapons* in law enforcement to avoid unnecessary harm and build trust,

Taking into consideration its resolution 50/21 to outline tools and principles for law enforcement officials managing peaceful assemblies,

Considering national security is defined as a state's ability to provide protection and defense to its citizens, according to the United Nations Office for the Coordination of Humanitarian Affairs (OCHA),

Acknowledging that human rights protestors are often targeted during their involvement in assemblies as per its resolution 56/10,

Noting that the OHCHR Model Protocols and Toolkits suggested by its resolution 55/60 provide guidelines to the management of peaceful assemblies,

Keeping in mind that the *Guidance on Less-Lethal Weapons in Law Enforcement* (2020) describes lethal weapons as equipment that can potentially lead to serious injuries, harm, or death,

Recalling the findings of the OHCHR report (A/HRC/50/42), which underscores the need to safeguard the rights to peaceful assembly and freedom of expression during times of crisis, including pandemics, security emergencies, and natural disasters, and emphasizing that such crises must not be used as a pretext for restricting fundamental freedoms,

1. *Recommends* the Special Rapporteur on freedom of peaceful assembly and of association to make recommendations with the purpose of improving national policies and aligning them with the ICCPR and the UDHR, following priorities such as:

    a. Leveraging governmental initiatives to establish channels which include, but isn't limited to, town halls and legislative sessions to involve civil societies in the policy-making process and overall civic and political spaces;

    b. Promoting the rights to assembly and protests, and focusing on de-escalation measures such as verbal dialogue and persuasion only when the assemblies infringe on national security;

    c. Developing law enforcement capacity building and training to avoid the use of lethal force and unlawful detentions during peaceful protests aligned with the Guidance on Less-Lethal Weapons in Law Enforcement (2020);

    d. Suggesting that national law enforcement not overuse their power, but rather aim to enforce a safe and peaceful assembly;

2. *Recommends* the Special Rapporteur on the freedom of peaceful assembly and of association to generate a supplementary report to the Model Protocol, focusing on principles for the protection of data in assemblies, to ensure that it is safeguarded from unauthorised third-party access to protect identities and actions of human rights defenders;

3. *Welcomes* the support of non-governmental organizations (NGOs) that focuses on freedom of expression and assembly, police brutality reporting, and governmental suppression of rights, such as Amnesty International and Human Rights Watch, in order to reinforce research and report incidents to develop these advanced policies on appropriate actions to maintain during peaceful protests and assemblies;

4. *Promotes* the introduction of governmental actions for civic education courses, based on the Special Rapporteur recommendations, with objectives such as:

    a. Raising awareness of students and citizens regarding their rights to protest and assembly, stated in article 21 of the ICCPR;

    b. Encouraging Member States to regulate and support the right to peaceful assembly in accordance with national laws and international instruments such as Article 21 of the ICCPR, by streamlining

approval procedures, promoting dialogue between authorities and protest organizers, and applying existing frameworks like the United Nations Human Rights Guidance on Less-Lethal Weapons to ensure non-violent de-escalation methods;

c. Focusing on further explanation on how protests are approved, developed and turned to practice within the legal limits of the Member State in question and international instruments like the HRC report 41/41 on “Rights to freedom of peaceful assembly and of association and the HRC resolution 33/22” (2018), Guidelines for States on the effective implementation of the right to participate in public affairs and HRC’s Guidance on Less-Lethal Weapons in Law Enforcement;

d. Understanding the legal means such as trials, investigations, legal advisors, and processes of victim protection available to citizens if their rights are believed to have been violated;

5. *Further requests* fair legal protection for victims of rights violations during peaceful protests, by:

    a. Creating independent bodies at the national level to manage complaints on police forces and avoid corruption within the investigation;

    b. Recommending the provision of free legal aid to individuals arrested during peaceful protests, funded through government-supported legal aid programs or independent human rights organizations;

    c. Encouraging Member States to ensure swift, fair, and impartial judicial review of any such detention in their national legislative bodies and judicial courts;

    d. Evaluating national judicial systems, especially on the issue of legal protection for victims of rights violations during peaceful protests, in the Universal Periodic Review (UPR);

6. *Recommends* law enforcement authorities in Member States find ways to make public spaces safe during protests, by communicating with those organizing the protest and providing services like traffic management and access to first-aid services;

7. *Requests* that the OHCHR establish clear principles to ensure the Member States respect the privacy rights of the protesters, which include the protection of biometric data, digital footprints, identities, communications, and locations, such as:

    a. Refraining from the collection of protesters’ personal data;

    b. Specifying the purpose and the scope regarding the use of personal data if in urgent situations such as national emergencies or life-threatening incidents;

    c. Keeping the data for only a specific amount of time;

    d. Empowering citizens' rights to withdraw consent to the data usage;

8. *Calls upon* Member States to implement the recommendations outlined in HRC report 50/42, particularly by adopting legal and institutional safeguards that prevent the misuse of emergency powers to suppress peaceful protests, and by strengthening national accountability mechanisms, including:

    a. The establishment of independent oversight bodies;

    b. Transparent investigation procedures;

c. Judicial review systems that ensure that violations of human rights committed during assemblies are effectively addressed and that victims have access to justice and reparations.

Code: HRC/2/2
Committee: Human Rights Council
Topic: Safeguarding Human Rights in Peaceful Protests and Assemblies

---

The Human Rights Council,

Recalling article 21 of the *International Covenant on Civil and Political Rights* (ICCPR) (1966), which guarantees the right to peaceful assembly, and allows for restrictions to be prescribed by law as deemed necessary in the interests of national security, public safety, public order, or the protection of rights and freedoms,

Acknowledging Article 2.1 of the *Charter of the United Nations* (1945), which honors the sovereign equality of all Member States and emphasizes its importance when governing peaceful assembly laws worldwide,

Considering the report by the Office of the United Nations High Commissioner for Human Rights (OHCHR) (A/HRC/50/47), the right to peaceful protest is a key aspect of society, allowing people to express their dissatisfaction and urge governments to act,

Fully aware that the OHCHR is the leading human rights organization in the United Nations (UN) system and its mission is to protect human rights for all people, ensure compliance with and improve existing policies, respect and protect human dignity, and uphold people's human rights,

Reiterating regional frameworks such as the *African Charter on Human and Peoples' Rights* (Banjul Charter) (1979), which expresses the rights of liberty, security, free association, and assembly, and its subsequent *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, which created the African Court, under which the Member States are subject to a judiciary that reinforces and fosters the values of the Banjul Charter,

Having heard the regional frameworks, such as article 11 of the *European Convention on Human Rights* (ECHR) (1950), everyone has the right to freedom of peaceful assembly and freedom of association with others, and no restrictions shall be placed on it other than those prescribed by law and necessity to protect national security or public safety and order,

Noting the Crisis Intervention Team (CIT) as an international framework for law enforcement training prioritizing de-escalation and community management,

Recognizing its resolution 56/10, which encourages Member States to seek potential technical assistance from intergovernmental actors to assist in facilitating effective peaceful assemblies,

Concerned about the OHCHR report (A/HRC/50/42), which states that, instead of seeing protests as a means of political participation, governments too often resort to repression and violence against peaceful protesters,

Desiring Member States to prioritize dialogue and negotiations, including mediation, between assembly organizers and governments, facilitated by state-approved authorities,

Taking note of the ICCPR, which provides an overview of the right to peacefully assemble with emphasis on the restrictions highlighted in article 21 of the ICCPR and outlines the responsibilities of states and the mode of conduct of law enforcement agencies in ensuring the right to peacefully protest,

Commends General Assembly resolution 68/181, which calls upon Member States to implement Security Council resolutions on women, peace, and security, focusing on addressing the challenges that women human rights defenders face in accessing justice during armed conflict,

Appreciating the United Nations Development Programme's (UNDP) *Women Peace and Security Agenda*, which calls for Member States' support for women's equality and women's empowerment,

Gravely concerned that in May 2022 and April 2023 OHCHR documented 41 killings of women human rights defenders in conflict-affected countries, highlighting the severe risks they face,

1. *Encourages* the universal adoption of article 21 of the ICCPR by Member States in domestic legislation to ensure the implementation of the rights and duties of protesters and law enforcement;

2. *Asks* the OHCHR to establish a centralized digital compendium, which serves as a repository for easily accessible information on people's right to peaceful assembly, including international and national standards, best practices, and guidelines on the protection of HRs in peaceful protests and assemblies, contributed to voluntarily by Member States, United Nations special rapporteurs, civil society organizations, human rights defenders and underrepresented groups to ensure comprehensive and wide-scale representational accuracy;

3. *Suggests* Member States establish regional courts such as the African Court of Human Rights and Peoples' Rights and the European Court of Human Rights through multilateral development in order to refine and strengthen the values and policies of regional frameworks on human rights;

4. *Requests* Member States to develop national online platforms with the aim of providing demonstrators with legal information, such as laws surrounding peaceful assembly and emergency assembly resources, such as first responder contacts and direct access to emergency response services;

5. *Advocates* for the adoption of national legal standards that regulate law enforcement agencies' actions, ensuring that protests are managed with minimal use of force, in line with the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials (1990) and the Model Protocol for Law Enforcement Officials;

6. *Calls upon* Member States to provide state-administered programs, such as the Practical Toolkit for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, to promote specialized and continuous human rights training to law enforcement personnel, with particular emphasis on the use of force and first-aid assistance in times of necessity by the treatment of protesters, and the protection of the rights to freedom of expression and peaceful assembly;

7. *Invites* Member States to facilitate open lines of communication between assembly organizers and authorities, encouraging consensus between the government and assembly leaders by receiving direction from the *United Nations Guidance for Effective Mediation* and/or non-governmental organizations;

8. *Urges* Member States, in collaboration with actors such as the Special Rapporteur on the Right to Peaceful Assembly and Association, the Special Rapporteur for Human Rights Defenders, and regional human rights organizations that contain curated ordinances of expression, assembly, security, and associated based on regional adversities and political views, such as the ASEAN Intergovernmental Commission on Human Rights and the African Charter on Human and People's Rights, to establish National Action Plans or protocols for peaceful assemblies, ensuring this right for all citizens;

9. *Recalls* that underrepresented groups such as women, children, and people with disabilities have historically faced oppression and inequality, leading to their increased involvement in protests, and:

a. Encourages Member States to adopt specific policies to protect underrepresented groups;

b. Suggests immediate support services through national groups similar to Doctors Without Borders or the International Federation of Red Crescent Societies, such as medical aid, psychological first aid, trauma counseling, and legal assistance to those who may experience violence or harassment;

10. *Requests* that the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women) establish further training courses open to all women globally on their digital Training Centre, focusing on the right to peaceful assembly, ensuring all women are aware of their international and regional rights and protections for peaceful assembly.