ASIS MODEL UNITED NATIONS 2026

Al Saad Indian School, Al Ain

SOCHUM STUDY GUIDE

Committee	Social, Humanitarian and Cultural Committee (SOCHUM)
Agenda	Protecting Human Rights in the Digital Age: Safeguarding Biometric Privacy, Mass Surveillance Data, and the Right to Anonymity
Prepared by	ASIS MUN Policy Department

I. Introduction to the Committee

The Social, Humanitarian and Cultural Committee (SOCHUM) is the **Third Committee of the United Nations General Assembly**. Like all six main committees of the General Assembly, it includes all 193 Member States. It deals with social, humanitarian and cultural issues that affect people worldwide, and above all with human rights.

Mandate and purpose

SOCHUM discusses a wide range of issues, including the rights of women and children, Indigenous peoples, refugees, the elimination of racism, the right to self-determination and freedom of expression. It considers the reports of the Human Rights Council, established in 2006, and of the UN's special procedures, and recommends resolutions to the General Assembly plenary.

The main purposes of SOCHUM are to:

1. Identify global social and humanitarian challenges.
2. Discuss violations of human rights and propose solutions.
3. Draft resolutions and recommendations for adoption by the General Assembly.
4. Encourage cooperation among Member States, UN bodies and civil society.
5. Protect marginalised and vulnerable communities.
6. Promote equality, dignity, peace and social progress.

II. Understanding the Agenda

A. Definition and Scope

The agenda concerns the responsibility of governments, technology companies and other organisations to protect people's fundamental rights when they collect, store, analyse or share digital information. It is based mainly on the **right to privacy**, recognised in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Privacy also supports freedom of expression, peaceful assembly and association, equality and human dignity.

B. Biometric Privacy

Biometric data are biological or behavioural characteristics that can identify a person, such as fingerprints, facial features, iris and retina patterns, DNA, voice and gait. Biometric data are extremely sensitive because they are permanently linked to a person and cannot be replaced if stolen.

- **Risks:** permanent identity exposure, unclear consent, "function creep" (data collected for one purpose being used for another), misidentification and discrimination.
- **Safeguards:** biometric systems should be used only for a clearly defined, lawful purpose, with strict laws, oversight and remedies when data are misused.

Facial Recognition Technology (FRT) compares an image of a person's face with a database of known images and records. States and private actors increasingly use biometric technologies to analyse how people look, act and express themselves, from border control to unlocking smartphones. When misused, these technologies can profile and categorise people by age, gender or skin colour, reinforcing discrimination against groups that have historically been excluded. Civil society organisations such as

ARTICLE 19 have called for a moratorium on the development and deployment of biometric surveillance technologies until adequate human rights safeguards are in place.

C. Mass Surveillance and Surveillance Data

Mass surveillance is the large-scale, generalised collection, interception and storage of information, often without individual suspicion. It may involve calls, messages, emails, browsing history, location data, CCTV footage, social media activity or facial recognition.

Surveillance data include both the content of communications and **metadata**, such as who contacted whom, when, and from where. Metadata alone can reveal a person's habits, relationships, movements and beliefs.

- **Modern surveillance technology:** CCTV networks are now common in cities worldwide and are increasingly combined with facial recognition and algorithms that analyse behaviour in real time. Drones, GPS trackers and mobile phone tracking tools allow people's movements to be followed with high precision.
- **Security benefits:** surveillance can deter some crimes, provide evidence for investigations, help police respond faster, improve safety in public spaces and help detect terrorist threats or cyberattacks. Its effectiveness depends on how it is used, and research suggests it can sometimes displace crime rather than reduce it.
- **Risks:** unauthorised data sharing, data breaches, racial or ethnic profiling, false accusations based on automated systems, and a "chilling effect" on free expression.
- **The key test:** under international human rights law, surveillance must be **lawful, necessary, proportionate**, targeted where possible, and subject to independent oversight. Governments should not collect everyone's data simply because technology makes it possible.
- **Consent:** people are often monitored without being informed and cannot realistically refuse surveillance in public spaces, workplaces, online platforms or essential services.

D. The Right to Anonymity

The right to anonymity is the ability to communicate, access information, take part in public life and express opinions without being forced to reveal one's identity. Anonymity protects journalists, whistleblowers, activists, human rights defenders, minorities and people seeking sensitive health or legal information. Encryption and anonymity tools help protect both privacy and freedom of expression (UN Special Rapporteur, A/HRC/29/32, 2015).

- **Concerns:** anonymity can be misused for cyberbullying, fraud, hate speech, terrorist recruitment, child exploitation and harassment.
- **Balance:** human rights bodies recommend that states protect strong encryption and anonymity, and restrict them only through targeted, lawful measures rather than blanket bans or weakened security for everyone.

E. Protecting Human Rights Defenders in the Digital Age

In April 2025, the **Human Rights Council** adopted **resolution 58/23**, "Human rights defenders and new and emerging technologies: protecting human rights defenders, including women human rights defenders, in the digital age", without a vote. It calls on states to protect defenders online and offline, including activists, women human rights defenders, environmental and Indigenous defenders, journalists, lawyers and their families, and not to use laws or administrative measures to block their access to funding, platforms and networks.

Agenda area	How HRC resolution 58/23 connects
Biometric privacy	Seeks to prevent emerging technologies from being used against activists and vulnerable groups.
Mass surveillance data	Opposes unlawful monitoring, spyware and technology-enabled attacks.
Right to anonymity	Supports secure, confidential communication for defenders, journalists and whistleblowers.
Freedom of expression	Protects people who criticise governments or expose abuses.
Non-discrimination	Gives special attention to women, Indigenous and environmental defenders and vulnerable groups.
Accountability	Calls for independent investigations and justice for victims.

III. Major Conventions and Legal Frameworks

- **Universal Declaration of Human Rights (UDHR, 1948), Article 12:** protects against arbitrary interference with privacy, family, home or correspondence.
- **International Covenant on Civil and Political Rights (ICCPR, 1966), Article 17:** the main treaty basis for the right to privacy; Article 19 protects freedom of expression. UN resolutions repeatedly affirm that these rights apply online as well as offline.
- **European Convention on Human Rights (1950), Article 8:** the provision used by the European Court of Human Rights to scrutinise surveillance and data retention.
- **American Convention on Human Rights (1969), Article 11**, and the **African Charter on Human and Peoples' Rights (1981)**, which regional bodies increasingly apply in digital contexts.

IV. Past Action

- **General Assembly resolution 68/167 (2013), "The right to privacy in the digital age":** adopted after revelations of large-scale surveillance, it affirmed that the same rights people have offline must be protected online. The Assembly has adopted follow-up resolutions regularly since.
- **OHCHR report A/HRC/27/37 (2014):** the first UN report on the right to privacy in the digital age.
- **Special Rapporteur on the right to privacy (2015):** a mandate created by the Human Rights Council to monitor and report on privacy worldwide.
- **Special Rapporteur report A/HRC/29/32 (2015):** on encryption and anonymity in digital communications.
- **Special Rapporteur report A/HRC/38/35 (2018):** on human rights and the regulation of online content.
- **Human Rights Council resolution 58/23 (2025):** on protecting human rights defenders in the digital age.

V. Regional Positions

Europe (Council of Europe and European Union)

- **Council of Europe Convention 108 (1981):** the only binding international treaty on data protection, with more than 50 parties, including some states outside Europe. Its modernised version, **Convention 108+**, adds specific safeguards for biometric data and is in the process of ratification.
- **Guidelines on Facial Recognition (2021)** under Convention 108 set reference measures for governments and companies.
- **Framework Convention on Artificial Intelligence (2024):** the first binding international treaty on AI, requiring human rights safeguards, transparency and oversight for AI systems, including AI-driven surveillance.
- **EU General Data Protection Regulation (GDPR):** treats biometric data used for identification as a special category of data subject to strict conditions.
- **EU AI Act (2024):** prohibits certain uses, such as social scoring and untargeted scraping of facial images, and strictly limits real-time remote biometric identification by police in public spaces.
- **Courts:** the European Court of Human Rights and the Court of Justice of the EU have set limits on bulk interception and mass data retention.

Africa

- **Malabo Convention (African Union Convention on Cyber Security and Personal Data Protection, 2014):** entered into force in 2023 and provides a regional baseline for data protection, including rules on biometric data.
- **African Declaration on Internet Rights and Freedoms:** a civil society declaration that recognises the right to anonymous communication and to the protection of personal information online.
- **East African Community:** has developed a regional framework encouraging member states to adopt data protection laws.
- Although the African Charter has no explicit privacy clause, the African Commission increasingly interprets other rights in ways that limit arbitrary surveillance.

Americas

- **American Convention on Human Rights, Article 11:** explicitly protects privacy and is applied by the Inter-American Court of Human Rights.
- **OAS Principles on Privacy and Personal Data Protection:** regional soft-law standards similar to Convention 108 and the GDPR.
- **Ibero-American Data Protection Standards:** align with GDPR-style protections for biometric and sensitive data.

Arab region and Middle East

There is no binding regional treaty on data protection or digital rights comparable to Convention 108 or the Malabo Convention. Gulf Cooperation Council states, including the UAE and Saudi Arabia, have adopted national data protection laws in recent years, often influenced by the GDPR, while regional approaches to surveillance are shaped largely by security and counter-terrorism cooperation.

Asia and ASEAN

ASEAN has adopted non-binding frameworks on personal data protection, but Asia has no regional human rights court or binding regional treaty on surveillance. Standards are driven mainly by national laws, such as India's Digital Personal Data Protection Act (2023) and China's Personal Information Protection Law (2021).

Cross-regional dialogue

The European, Inter-American and African human rights courts maintain a Permanent Forum of Institutional Dialogue, created by the San José Declaration (2018), which allows them to exchange approaches on issues including privacy and new technologies.

Key actors

Country	Points to research
United States	No single federal privacy law; major home of technology companies and of large-scale intelligence surveillance programmes.
China	Extensive state surveillance, including facial recognition, alongside its Personal Information Protection Law (2021).
Russian Federation	Uses facial recognition widely in public spaces and prioritises state security and "digital sovereignty".
Germany and France	EU members bound by the GDPR and the AI Act; strong advocates of data protection.
United Kingdom	Council of Europe member with its own data protection law; uses live facial recognition in policing.
India	Runs the world's largest biometric ID system, Aadhaar, and adopted the Digital Personal Data Protection Act (2023).
Brazil	Its General Data Protection Law (LGPD) is modelled on the GDPR.
Saudi Arabia and the United Arab Emirates	National data protection laws alongside a strong emphasis on security.
South Africa	Its Protection of Personal Information Act (POPIA) is one of Africa's most developed data protection laws.

VI. Key Challenges

1. **Technology moves faster than law:** biometric systems, AI-driven surveillance and data aggregation evolve faster than treaties and national laws can be updated.
2. **Biometric data cannot be reset:** unlike passwords, compromised biometric traits are compromised for life, enabling identity theft and long-term tracking.
3. **Algorithmic bias:** facial recognition systems trained on unrepresentative data show higher error rates for some demographic groups, leading to wrongful identification and discriminatory policing.

4. **Security versus rights:** states justify broad surveillance powers on grounds of counter-terrorism, border control and public order, while critics argue these measures are disproportionate and undermine democracy.
5. **The role of companies:** much surveillance technology is designed, sold and operated by private companies, including spyware vendors, which are harder to hold accountable under international law.

VII. Possible Areas of Debate

1. Is bulk or indiscriminate digital surveillance ever compatible with human rights law, and if so, under what safeguards?
2. Should anonymity and strong encryption be recognised as rights in themselves, or are they sufficiently protected as part of privacy and freedom of expression?
3. How should responsibilities be divided between states and technology companies, especially in public-private partnerships?
4. How can states balance the benefits of digital ID and biometric registration, such as access to services and financial inclusion, against the risks of exclusion and surveillance?
5. Should there be a moratorium on facial recognition in public spaces, or on the sale of spyware, until safeguards are in place?
6. What protections are needed for journalists, activists and human rights defenders who face digital surveillance?

VIII. Guiding Questions

1. What legal, technical and organisational safeguards would ensure that biometric systems comply with the principles of legality, necessity, proportionality and non-discrimination?
2. What oversight mechanisms, such as judicial authorisation, independent auditors and public reporting, are essential to prevent abuse of surveillance powers?
3. How can anonymity tools be protected while still allowing lawful, targeted investigations of serious crime?
4. What role should regional human rights courts and bodies play in harmonising standards across jurisdictions?
5. What is your country's own record on surveillance and data protection, and how does it shape your position?

IX. Key Terms

Term	Meaning
Biometric data	Physical or behavioural characteristics that can identify a person, such as fingerprints, face or voice.
Facial Recognition Technology (FRT)	Software that identifies or verifies people by comparing images of their faces with a database.
Mass surveillance	Large-scale, indiscriminate monitoring of a population rather than targeted individuals.
Metadata	Information about communications, such as sender, recipient, time and location, rather than content.
Function creep	The use of data or technology for purposes beyond those for which it was originally collected.
Encryption	Encoding information so that only authorised people can read it.
Anonymity	Acting or communicating without revealing one's identity.
Spyware	Software used to secretly access and monitor a person's device.
Necessity and proportionality	The tests that any limitation on a human right must meet under international law.
Human rights defender	Any person who, individually or with others, works to promote or protect human rights.

X. Committee Procedure

- This committee follows the **ASIS MUN 2026 Rules of Procedure (ROP)**. Where this guide and the ROP differ, the ROP applies.
- **Position papers** are compulsory and must be submitted to the Executive Board during the **first committee session**. Maximum two pages, excluding the bibliography, in the format given in **Appendix A of the ROP**. Wikipedia must not be cited.
- **Working papers** may have up to 5 authors and are voted on by simple majority. Only a passed working paper can be developed into a draft resolution.
- **Draft resolutions** may have a maximum of **3 authors per bloc** and must follow the format in **Appendix C of the ROP**. The committee opening line is *The Social, Humanitarian and Cultural Committee,*
- **Voting on draft resolutions:** a draft resolution passes with a **two-thirds majority of Yes over No votes** (abstentions are not counted), unless the Chair announces a different threshold before voting procedure. Draft resolutions are voted on by roll call.
- **Mandate:** as the Third Committee of the General Assembly, SOCHUM adopts recommendations, not binding laws. Resolutions may call on states, encourage companies to respect human rights, request reports from UN bodies and propose standards, but cannot impose sanctions.

- **Use of AI** by delegates is allowed but results in a deduction of marks, with a greater deduction for paperwork.

XI. Conclusion

Protecting human rights in the digital age requires more than updating old privacy rules. It demands a rethink of how power operates when identity itself becomes data. Biometric systems, mass surveillance and the erosion of anonymity are not merely technical issues: they reshape the balance between state authority and individual freedom, and between security and democratic accountability. Delegates should recognise the particular risks of these technologies, including irreversible harm, discrimination and chilling effects on expression and association; turn existing human rights principles into concrete, enforceable limits with strong oversight and remedies; and treat anonymity and encryption as essential safeguards, especially for those whose safety depends on them. The foundations already exist in the instruments described in this guide. What remains is the political will to apply them, close the gaps, and hold both states and companies accountable.

XII. References

1. Universal Declaration of Human Rights (1948). https://www.un.org/en/about-us/universal-declaration-of-human-rights
2. International Covenant on Civil and Political Rights (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
3. OHCHR (2014), The Right to Privacy in the Digital Age, A/HRC/27/37. https://www.ohchr.org
4. UN General Assembly (2013), Resolution 68/167, The right to privacy in the digital age. https://digitallibrary.un.org
5. UN Special Rapporteur on Freedom of Expression (2015), Report on encryption and anonymity, A/HRC/29/32. https://www.ohchr.org
6. UN Special Rapporteur on Freedom of Expression (2018), A/HRC/38/35. https://www.ohchr.org
7. Human Rights Council (2025), Resolution 58/23. https://digitallibrary.un.org/record/4080898
8. Council of Europe, Convention 108 and Convention 108+. https://www.coe.int
9. Council of Europe, Framework Convention on Artificial Intelligence (2024). https://www.coe.int
10. European Union, Artificial Intelligence Act. https://eur-lex.europa.eu
11. ARTICLE 19, Biometric technologies and the right to anonymity. https://www.article19.org
12. Amnesty International, Encryption: A matter of human rights. https://www.amnesty.org

Note on the preparation of this guide

Artificial intelligence (AI) tools were used in the preparation of this study guide. The content has been reviewed by the ASIS MUN Policy Department, but delegates should verify key facts and figures against the original sources before using them in debate or in their position papers.

If you find any errors, please email **asis.mun@student.bhavansalain.com**.