

SYNOPSIS

HUMAN RIGHTS I

Chairs: Meda Folprechtová, Eva Nováková, Emma Werbiková

Topic:

Balancing counter-terrorism measures with civil liberties, with focus on the so-called “chat control”

Background Information

Terrorism has remained a significant global security concern over the past decades, prompting states to adopt increasingly advanced counter-terrorism strategies. As communication has largely shifted to digital platforms, terrorist organizations have adapted by using encrypted messaging services, social media, and private online networks to recruit members, spread extremist ideologies, and plan attacks. In response, governments have sought new methods to monitor online spaces and identify potential threats at an early stage.

One such method is the so-called “chat control,” a term used to describe policies that allow or require the monitoring or scanning of private digital communications. These measures may involve content scanning, metadata analysis, or the use of automated tools to detect suspected terrorist or extremist material. Chat control has been proposed or implemented in various forms across different regions, often justified as a necessary response to the challenges posed by encryption and anonymous online communication.

While these measures aim to strengthen public security, they have sparked widespread debate due to their impact on human rights. The right to privacy is protected under international law, and any interference with private communications must meet strict legal standards. Critics argue that broad surveillance measures risk violating these protections, especially when monitoring is conducted on a large scale rather than through targeted investigations. Concerns have also been raised about freedom of expression, as individuals may feel discouraged from speaking openly online if they believe their communications are being monitored.

The use of artificial intelligence and automated systems in chat control has further intensified these concerns. Automated tools are often unable to fully understand context, satire, or cultural differences, increasing the risk of false positives. This may result in innocent individuals being flagged for suspicious activity, leading to unnecessary investigations or restrictions. Minority and marginalized communities are often more vulnerable to these outcomes, particularly when biases are embedded within algorithms or data sets.

Another key challenge lies in oversight and accountability. In many cases, the legal frameworks governing digital surveillance remain unclear or underdeveloped. Questions persist regarding who authorizes surveillance measures, how long data is stored, how it is protected, and how individuals can seek redress if their rights are violated. Additionally,

digital communications frequently cross national borders, complicating issues of jurisdiction, data sharing, and international cooperation.

As states continue to search for effective ways to counter terrorism in the digital age, the debate over chat control highlights the need to carefully balance security objectives with the protection of fundamental rights. Understanding this background is essential for delegates as they work toward solutions that address both public safety and the preservation of civil liberties.

UN Involvement

The United Nations plays an important role in addressing terrorism while promoting respect for human rights. Through the General Assembly and the Security Council, the UN has adopted resolutions calling on states to prevent and combat terrorism, while emphasizing that all counter-terrorism measures must comply with international human rights law.

The Office of the United Nations High Commissioner for Human Rights (OHCHR) has raised concerns about mass surveillance and digital monitoring, warning that such practices may violate the right to privacy if they are not lawful, necessary, and proportionate. Similarly, the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism has highlighted the risks posed by new surveillance technologies and has called for stronger safeguards and oversight.

The Human Rights Council has also addressed the right to privacy in the digital age, affirming that human rights apply both online and offline. Overall, the UN encourages states to balance security needs with the protection of fundamental rights, providing a key framework for discussions on chat control and civil liberties.

Bloc positions

Delegates' positions on chat control and counter-terrorism measures generally fall into four main groups. Security-oriented states, including China, Russia, Türkiye, Egypt, Saudi Arabia, and Israel, prioritize national security and often support expanded surveillance powers, viewing human rights concerns as secondary to preventing attacks. Human rights-focused states, such as Germany, Norway, Sweden, the Netherlands, Canada, and New Zealand, emphasize privacy, freedom of expression, and strict limits on surveillance, opposing mass or indiscriminate monitoring and favoring targeted, court-approved measures. Balanced or middle-ground states, including France, the United Kingdom, Spain, Italy, Japan, and South Korea, seek compromise solutions that allow counter-terrorism measures only when paired with clear legal frameworks, independent oversight, and strong safeguards. Finally, developing or capacity-limited states, such as Nigeria, Kenya, Pakistan, Indonesia, Bangladesh, and the Philippines, focus on stability, international cooperation, and capacity-building, supporting counter-terrorism efforts while remaining cautious of complex or costly digital surveillance systems and their potential human rights impact.

Questions to consider

- What is my country's approach to counter-terrorism and digital surveillance?
- How does my country balance security measures with protecting privacy, freedom of expression, and personal data?
- What laws, oversight mechanisms, or safeguards does my country have to prevent abuse of surveillance tools, and could similar measures be applied internationally?
- How does my country use technology like AI in monitoring communications, and what steps are taken to avoid bias or targeting of vulnerable groups?