Advance edited version

Distr.: General
13 August 2026

Original: English

Advance edited version

Human Rights Council
Sixty-third session
7 September–9 October 2026
Agenda items 2 and 3
Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Terrorism and human rights

Report of the United Nations High Commissioner for Human Rights*

Summary

In the present report, the United Nations High Commissioner for Human Rights examines key developments at the intersection of terrorism, counter-terrorism and the right to privacy during the period July 2024 to June 2026. The High Commissioner analyses patterns in the use of data-driven, technology-enabled and administrative counter-terrorism measures and their implications for the right to privacy and related rights and recommends legislative, institutional and policy measures to strengthen safeguards, oversight and accountability in line with international human rights law.

* The present document was submitted to the conference services for processing after the deadline for technical reasons beyond the control of the submitting office.

I. Introduction

1. The present report is submitted pursuant to Human Rights Council resolution 57/11, on terrorism and human rights. In that resolution, the Council urged States to respect and protect the right to privacy, including in the context of digital communication, and to take measures to ensure that any interference with the right to privacy in counter-terrorism contexts was regulated by law and was consistent with the principles of legality, necessity and proportionality.

2. Terrorism has profound and far-reaching consequences for the enjoyment of human rights. Beyond immediate loss of life and physical integrity, terrorist acts cause long-term social, psychological and economic harm, displace communities, disrupt access to essential services, undermine social cohesion and development and may disproportionately affect already marginalized groups.

3. States must respond to these threats to human rights through comprehensive measures that themselves respect human rights, including through the adoption of a victim-centred approach that promotes access to justice, remedy, reparation and meaningful participation. In practice, however, States' responses to terrorism have not always met this standard. The early 2000s marked a turning point, with the rise of significant executive powers, mass surveillance and erosion of legal safeguards, a trajectory that technological developments have since deepened. Across regions, preventive and risk-based approaches have expanded, including the use of administrative measures, financial restrictions, travel bans and intelligence-led practices.[1] In many contexts, these measures are deployed without adequate oversight, transparency or accountability, and applied in ways that go beyond demonstrable security need. Where terrorism-related definitions are vague or overly broad, such measures may also facilitate the misuse of the label "terrorist", placing individuals outside ordinary legal protections.[2]

4. In this context, rapid technological developments are reshaping terrorist threats and State responses. The growing use of digital surveillance systems, large-scale data processing, biometric identification and artificial intelligence in counter-terrorism operations raises important questions regarding privacy, non-discrimination, procedural safeguards and access to remedy. These concerns are heightened in cross-border settings, where intelligence-sharing and joint operations frequently occur through opaque mechanisms that may fall beyond effective judicial or parliamentary oversight. In addition, digital platforms are being exploited to spread violent or terrorist narratives, while also serving as platforms for preventive measures, including monitoring and content moderation. In this evolving context, the right to privacy is a critical concern, not only as a right in itself but as an enabler for the exercise of other fundamental freedoms.

5. The present report is informed by submissions from stakeholders following a call for input in February 2026,[3] by previous reports by the Office of the United Nations High Commissioner for Human Rights (OHCHR) and United Nations human rights mechanisms, and by academics' and practitioners' research.

Advance edited version

[1] A/80/284, paras. 2, 10 and 17.

[2] A/HRC/61/52, paras. 3 and 5; and Office of the United Nations High Commissioner for Human Rights (OHCHR), *Fact Sheet No. 32: Human Rights, Terrorism and Counter-Terrorism*, revised ed. (New York and Geneva, 2025), pp. 21–23.

[3] All submissions, unless marked confidential, are available on the OHCHR website, at https://www.ohchr.org/en/calls-for-input/2026/call-inputs-report-terrorism-and-human-rights-will-be-presented-human-rights.

II. Impact of terrorism on the right to privacy

6. Terrorism has direct and serious consequences for the enjoyment of human rights, affecting not only the rights to life and security but also other rights, including the right to privacy.[4] The right to privacy is affected by terrorism in several distinct and interconnected ways.

7. Terrorist and violent extremist groups increasingly employ digital tools to obtain, exploit or weaponize personal data. Technologies that serve legitimate purposes, including social media platforms and communications tools, are exploited for recruitment, incitement and coordination.[5] In some contexts, terrorists and violent extremists use dark-web platforms and so-called cybercrime-as-a-service tools to gain access to sensitive personal information, compromise digital devices and facilitate cyberattacks against individuals and institutions.[6] These practices compromise personal data and raise concerns for the right to privacy.

8. The use of commercially available drone technology by terrorist and violent extremist groups[7] may also create risks to privacy. The Analytical Support and Sanctions Monitoring Team has documented how terrorist groups, including affiliates of Da'esh and Al-Qaida, have acquired and deployed drone systems for surveillance and reconnaissance purposes,[8] raising serious questions about the adequacy of existing legal and regulatory frameworks governing the commercial availability, acquisition and transfer of drone technology.

9. In today's increasingly digital environment, public institutions and many essential services rely on communications networks and data systems that handle personal information. When such systems are disrupted or compromised, personal data becomes vulnerable to exposure, loss or manipulation.[9] The increasing exploitation of information and communications technology by terrorist and violent extremist groups[10] allows them to take advantage of such vulnerabilities, further increasing risks to privacy and, by extension, to other human rights.

10. Terrorism can also compel people to flee their homes, making it a key driver for forced displacement.[11] Forcibly displaced persons may be required to disclose highly sensitive personal or biometric data during registration, often with limited information about how that data will be used or protected, without informed consent and with no option to withhold consent, out of fear or because of the risk of not obtaining a service if they do so. If these data are inadequately protected, individuals may be exposed to serious risks, including threats to physical integrity, legal status and access to services.[12] These concerns are heightened in situations where institutional safeguards are weak or data-protection systems have been compromised, including in contexts affected by terrorism, armed conflict or other situations of violence.

Advance edited version

[4] OHCHR, *Fact Sheet No. 32*, pp. 4 and 11.
[5] Delhi Declaration on countering the use of new and emerging technologies for terrorist purposes, paras. 4 and 5.
[6] United Nations Counter-Terrorism Centre and United Nations Interregional Crime and Justice Research Institute, Beneath the Surface: Terrorist and Violent Extremist Use of the Dark Web and Cybercrime-as-a-Service *for Cyberattacks* (New York and Turin, 2024), pp. 22, 26, 29 and 30.
[7] A/HRC/52/39, para. 37; and S/2025/482, para. 127.
[8] S/2025/482, paras. 72, 124, 127 and 128.
[9] A/HRC/60/45, paras. 2 and 29.
[10] Security Council Committee established pursuant to resolution 1373 (2001) concerning counter-terrorism (Counter-Terrorism Committee), "Information and communications technologies". Available at https://www.un.org/securitycouncil/ctc/content/information-and-communications-technologies.
[11] OHCHR, "UN expert urges protection of victims forcibly displaced by terrorism and counter-terrorism", 21 August 2025; and General Assembly resolution 71/1, para. 64.
[12] A/HRC/60/45, paras. 21 and 30.

III. Counter-terrorism and the right to privacy

A. Data-driven and technology-enabled counter-terrorism measures

11. The growing use of data-driven and technology-enabled measures in counter-terrorism has expanded States' capacity to monitor individuals and populations, raising concerns regarding the right to privacy when implemented without adequate safeguards. These concerns have grown as States across regions expand counter-terrorism measures in ways that enable increasingly intrusive interference with personal data.[13]

12. These counter-terrorism measures span a wide range of techniques, including surveillance and monitoring, biometric data collection, search and seizure powers and reporting to police.[14] Techniques such as facial recognition, smart-city systems and extensive online tracking are increasingly used, yet often operate without the legal safeguards, transparency or oversight required by international human rights standards.[15] Moreover, the use of biometric data and biometric technologies, such as fingerprinting and facial recognition, has expanded significantly,[16] and artificial intelligence and machine learning systems are now used in many counter-terrorism practices, including predictive threat assessment and large-scale data analytics.[17]

13. Surveillance measures introduced as counter-terrorism measures have contributed to blurring the lines between surveillance conducted for law enforcement purposes and intelligence-gathering.[18] Digital surveillance infrastructures, particularly those embedded in smart-city environments, enable continuous monitoring of public spaces and facilitate the collection of data on individuals' movements, interactions and behaviour in ways that go beyond original law enforcement or counter-terrorism purposes.[19]

14. The risks associated with data retention are especially acute with respect to biometric information. Biometric data collected for counter-terrorism purposes may be retained and shared among intelligence, law enforcement and border management authorities, including through interoperable databases.[20] Such practices are not always accompanied by clear legal frameworks, regulating the retention of, access to or the further use of the collected data.[21] Given the permanent nature of biometric identifiers, shortcomings in data-protection frameworks increase the risk of long-term consequences, such as persistent surveillance, misidentification or discriminatory profiling, particularly for individuals and groups subject to increased security screening.[22]

---

[13] A/HRC/55/48, para. 10; Counter-Terrorism Committee Executive Directorate, "CTED analytical brief: biometrics and counter-terrorism" (2021), pp. 4–6; and OHCHR, *Fact Sheet No. 32*, pp. 49–53.

[14] A/80/284, para. 10.

[15] A/HRC/60/45, paras. 19 and 31; and OHCHR, *Fact Sheet No. 32*, pp. 53 and 54.

[16] Counter-Terrorism Committee Executive Directorate, "CTED analytical brief", pp. 1 and 4; OHCHR, *Fact Sheet No. 32*, pp. 53 and 54; and Committee on the Elimination of Racial Discrimination, general recommendation No. 36 (2020), para. 35. See also Security Council resolution 2396 (2017), para. 15.

[17] Counter-Terrorism Committee Executive Directorate, "CTED analytical brief", p. 4; and OHCHR, *Fact Sheet No. 32*, pp. 53 and 54.

[18] A/HRC/57/29, para. 24; and OHCHR, *Fact Sheet No. 32*, p. 49.

[19] A/HRC/60/45, paras. 29–31; and OHCHR, *Fact Sheet No. 32*, p. 51.

[20] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of biometric data to identify terrorists: best practice or risky business?", University of Minnesota, July 2020 (available at https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf), pp. 8–10, 22, 23, 27 and 28. See also Security Council resolution 2396 (2017), paras. 13 and 15.

[21] Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "Protecting human rights while using artificial intelligence to counter terrorism: position paper", December 2025, p. 22.

[22] Panel for the Future of Science and Technology and European Parliamentary Research Service, *Person Identification, Human Rights and Ethical Principles: Rethinking Biometrics in the Era of Artificial Intelligence* (Brussels, European Union, 2021), pp. 27 and 33–35. See also CERD/C/GBR/CO/24-26, paras. 35 and 36.

Advance edited version

15. United Nations human rights mechanisms have raised concerns about the use of such technologies under counter-terrorism and national security mandates.[23] The Human Rights Committee expressed concern about reports indicating that surveillance activities in Canada had been significantly expanded for broadly defined "national security" purposes,[24] and about the reported use of spyware in Spain to monitor politicians, activists and public figures between 2017 and 2020, urging the State to ensure that all forms of surveillance and interference with privacy were in full compliance with article 17 of the International Covenant on Civil and Political Rights.[25] OHCHR likewise noted that intrusive surveillance measures, such as biometric recognition systems, digital tracking and mass data processing, could operate with limited transparency or independent oversight, increasing the risk of discriminatory surveillance and unlawful interference with privacy.[26]

16. The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has warned that data sets and algorithms may be biased or inaccurate, potentially leading to discriminatory profiling, violations of the right to privacy and counterproductive false positives.[27] In Myanmar, OHCHR has observed that the creation of a nationwide integrated biometric system covering the entire population of Myanmar, justified on grounds of national security and crime prevention, raises serious human rights concerns, particularly regarding privacy and the absence of adequate data-protection safeguards, in a context of diminished rule of law since the military coup of 2021.[28]

17. Information gathered by OHCHR, together with submissions from civil society, has indicated that surveillance, financial monitoring and the designation of individuals as terrorist actors or otherwise subjecting them to security listing or profiling introduced under counter-terrorism or counter-extremism legislation are frequently applied through administrative procedures based on undisclosed intelligence.[29] In the Russian Federation, 20,813 individuals had been placed on the national "list of terrorists and extremists" by April 2026, enabling the authorities to freeze bank accounts without a court order, with implications for a range of human rights, including the right to privacy.[30]

18. In the Bolivarian Republic of Venezuela, OHCHR observed that, following the elections in July 2024, the authorities promoted the use of a citizen-reporting application, authorized inspections of mobile phones by State security actors and disseminated videos, digitally edited images and personal data of detained individuals on social networks. Amid geopolitical tensions with the United States of America in September 2025, the authorities sought to revive the application to facilitate citizen reporting of suspected dissidents. In Côte d'Ivoire, OHCHR also observed that biometric registration of refugees conducted under counter-terrorism frameworks raised concerns about the risk of ethnic stigmatization and the absence of adequate data-protection safeguards.

B. Governance of counter-terrorism measures and accountability deficits

19. Beyond the proliferation of surveillance and data-driven technologies, serious concerns arise regarding governance frameworks – or the absence thereof – within which such technologies are developed, deployed and overseen. In particular, the increasing reliance on administrative measures, automated systems and public-private cooperation in counter-terrorism contexts raises questions regarding accountability, oversight and the effective protection of the right to privacy.

[23] For example, A/HRC/52/39, para. 9.
[24] CCPR/C/CAN/CO/7, para. 23.
[25] CCPR/C/ESP/CO/7, paras. 40 and 41.
[26] A/HRC/60/45, paras. 19 and 31; and A/HRC/27/37, paras. 37, 38 and 48–50.
[27] "Protecting human rights while using artificial intelligence to counter terrorism", p. 1.
[28] Ibid., p. 5.
[29] See submissions from World Organisation against Torture, National Union of Peoples' Lawyers of the Philippines and MENA Rights Group.
[30] A/80/382, paras. 38–40; and OHCHR, "Strategy of blatant abuse of counter-terrorism and extremism laws to destroy Russian civil society must end: UN experts", 9 April 2026.

Advance edited version

20. International human rights law requires that any interference with the right to privacy be authorized by law, pursue a legitimate aim and be necessary and proportionate. A decision to make use of such authorized interference must be made on a case-by-case basis and only by the authority designated under the law,[31] and any interference must be subject to independent oversight, judicial safeguards and effective remedies.[32] By these standards, accountability frameworks and oversight mechanisms have not kept pace with the expansion of counter-terrorism measures.[33] Counter-terrorism frameworks may grant broad discretionary powers to executive authorities, including security and intelligence services, and may lack appropriate safeguards.[34] This increases the risk that personal data are collected, processed, shared or retained in ways that may amount to undue interference with the right to privacy.[35]

21. Automated content moderation presents a related but distinct accountability concern. Systems designed to detect or remove content labelled as "terrorist" or "extremist" frequently operate on the basis of inexact or overbroad labelling that goes beyond the essential components of terrorism-related offences without adequate transparency, notification or effective remedies to challenge decisions or obtain redress.[36] Private digital platforms often cooperate with State authorities in ways that blur the distinction between public sector surveillance and private data processing, which may also have implications for the right to privacy.[37]

22. Concerns regarding content moderation are compounded by expanding data ecosystems characterized by the interoperability of public and private databases.[38] Passenger data, financial information, social media data and other forms of behavioural data are increasingly aggregated and analysed across institutions and borders.[39] Without data-protection safeguards, including strict purpose limitation and data minimization requirements, such architecture facilitates function creep and blurs the boundaries between targeted investigation and pervasive population monitoring.[40]

23. Private companies warrant specific attention given their central and growing role in the development and operation of counter-terrorism technologies, including surveillance tools, content-moderation systems and data-analytics platforms, often without adequate oversight.[41] Given the substantial potential risks for human rights, businesses should, consistent with principles 15 (b) and 17 of the Guiding Principles on Business and Human Rights, conduct systematic human rights due diligence throughout the life cycle of counter-terrorism technologies. States, in turn, remain responsible for protecting human rights from violations by third parties and for ensuring that the involvement of private actors

[31] Human Rights Committee, general comment No. 16 (1988), para. 8.
[32] Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "Protecting human rights while using artificial intelligence to counter terrorism", p. 21.
[33] A/HRC/39/29, paras. 26 and 40; and A/HRC/52/39, paras. 43 and 50.
[34] A/HRC/27/37, para. 29; A/HRC/37/52, paras. 32 and 34; and OHCHR, *Fact Sheet No. 32*, p. 26.
[35] A/HRC/39/29, para. 21; A/HRC/40/63, para. 36; and A/HRC/52/39, paras. 26 and 50.
[36] European Union Agency for Fundamental Rights, Regulating Online Terrorist Content*:* Balancing Public *S*afety and Fundamental Rights (Luxembourg, Publications Office of the European Union, 2026), sects. 1.1, 3.1.1, 4.2 and 4.3; and OHCHR, *Fact Sheet No. 32*, p. 50.
[37] A/HRC/60/45, para. 45; OHCHR, "UN experts: safeguard human freedoms from systematic digital interference, surveillance and chilling effects on civic space", 27 April 2026; and Privacy International, "Safeguards for public-private surveillance partnerships", December 2021, p. 3. See also A/79/319, paras. 59 and 60.
[38] OHCHR and University of Essex, "Digital border governance: a human rights-based approach", September 2023, pp. 15 and 16; A/HRC/60/45, para. 21; and European Union Agency for Fundamental Rights, Interoperability and Fundamental Rights Implications*: Opinion of the European Union Agency for Fundamental Rights* (Vienna, 2018), pp. 7, 10 and 11.
[39] OHCHR and University of Essex, "Digital border governance", pp. 15 and 16; Security Council resolution 2396 (2017), paras. 12, 13 and 15; and A/HRC/60/45, para. 21.
[40] OHCHR, *Fact Sheet No. 32*, p. 51; A/HRC/51/17, para. 5; A/HRC/60/45, para. 30; and OHCHR and University of Essex, "Digital border governance", pp. 15 and 16.
[41] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (London, Chatham House, 2019), pp. 9 and 16–18; and A/HRC/52/39, paras. 44–48.

Advance edited version

in counter-terrorism does not result in arbitrary or unlawful interference with privacy.[42] Accordingly, States should ensure effective regulation and independent oversight of companies, including by making human rights due diligence mandatory in areas of heightened human rights risk.[43] Separately, States should also conduct due diligence through the life cycle of their own use of technologies related to counter-terrorism and guarantee accessible remedies for individuals affected by their use by States or companies.[44]

24. Accountability deficits also arise in connection with administrative counter-terrorism measures, such as restrictive orders, movement controls, terrorist listings and asset freezes, where proper oversight and remedies are not properly integrated. This includes situations where reliance on undisclosed intelligence is not subject to effective independent review and where the absence of effective judicial review and remedies can result in arbitrary interference with privacy and other rights.[45]

25. Additional concerns about transparency, due process guarantees and access to effective remedies arise from the deployment of artificial intelligence and algorithmic tools in counter-terrorism. These concerns are heightened by the probabilistic nature of many artificial intelligence systems, which may generate inaccurate or biased output when used for predictive assessment purposes. Predictive profiling may undermine the presumption of innocence and other fair trial rights when the basis for decisions cannot be understood or their accuracy or lawfulness effectively challenged. Without transparency, explainability and effective remedies, automated systems used in counter-terrorism risk reinforcing discrimination and enabling arbitrary interferences with privacy, including where data sets used to train such systems reflect existing biases or patterns of racial or other profiling, resulting in discriminatory outcomes that individuals have no meaningful way to identify or contest.[46]

26. Stakeholders, in their submissions, noted that accountability deficits in counter-terrorism frameworks were often structural. They reported that secrecy provisions, exemptions on grounds of national security and reliance on classified intelligence limited the ability of courts and oversight bodies to carry out meaningful review. Individuals subjected to surveillance or asset freezes were frequently unaware of the action taken against them, making access to effective remedies challenging.[47]

27. In its submission, one stakeholder reported that thousands of individuals listed as suspected terrorists in Tunisia by the Ministry of Interior had been subjected to several restrictions – including house arrest, travel bans, repeated police summons and home searches – reportedly without legal basis, written notification or effective judicial remedy, with severe psychological and social consequences for those affected and their families. According to the submission, the opaque nature of the listing system raised concerns, as the measures imposed could affect the right to private life and the inviolability of the home.[48]

28. Accountability deficits are further compounded by the cross-border dimension of contemporary counter-terrorism practices, which presents distinct challenges for the protection of the right to privacy, particularly where intelligence cooperation and data-sharing arrangements involve the transfer and use of personal data without adequate

[42] Guiding Principles on Business and Human Rights, principle 1 and the commentary thereto; and A/HRC/27/37, para. 43.

[43] Guiding Principles on Business and Human Rights, principles 1, 3, 4 and the commentaries thereto; and A/HRC/62/33, paras. 24, 25 and 37.

[44] A/HRC/62/33, paras. 22 and 44 (a) and (f); and OHCHR, "UN experts: safeguard human freedoms".

[45] A/80/284, para. 7 (c), (d) and (f). See also CCPR/C/ISL/CO/6, para. 29.

[46] Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "Protecting human rights while using artificial intelligence to counter terrorism", pp. 15 and 22–25.

[47] See submission from Human Rights Commission of Zambia and National Union of Peoples' Lawyers of the Philippines.

[48] See submission from World Organisation against Torture.

Advance edited version

safeguards or oversight. Intelligence cooperation, data-sharing arrangements and joint operations increasingly operate through opaque, informal or classified mechanisms, often beyond effective public scrutiny and judicial oversight.[49]

29. Domestic oversight bodies are often not equipped to oversee cross-border intelligence cooperation, owing to diverse factors, such as sovereignty constraints, limited access to intelligence-sharing agreements and the inability to verify how foreign partners collect, retain, process or use shared information. While the need-to-know principle and the policy of "originator control" that govern most intelligence-sharing arrangements can serve legitimate purposes, including protecting sensitive information and individual privacy, they also limit transparency and accountability when intelligence is shared across borders.[50] In particular, where information is exchanged with foreign partners without adequate safeguards, oversight or clear restrictions on its use, these practices can increase the risk of human rights violations.[51] Concerns have been raised that intelligence-sharing arrangements may operate without sufficiently clear legal frameworks, transparency or oversight.[52]

30. Personal communications data and bulk metadata may be exchanged without clear limits on use, retention or onward transfer, creating a significant risk of undue interference with the right to privacy.[53] An additional concern is that data shared between intelligence services may no longer be subject to the same sufficient and adequate safeguards once they reach the receiving State, as it may be unclear whether equivalent privacy and data-protection standards are maintained once the data are transferred to the receiving State.[54]

31. United Nations human rights mechanisms have expressed concern that transnational intelligence-sharing frameworks may enable States to circumvent domestic legal safeguards by obtaining or disseminating personal data through foreign partners,[55] including where such data could not lawfully be collected under domestic law. [56] Expert analysis has highlighted that such arrangements are frequently not grounded in law and operate on a classified basis, placing them beyond public scrutiny and preventing meaningful oversight of how personal data are collected, retained, shared and used across jurisdictions.[57] Telecommunications companies, digital platforms and financial institutions may be required to share personal data across jurisdictions,[58] often without adequate safeguards to prevent incompatible use or onward transfer, thereby increasing the risk of misuse and unlawful interference with privacy.[59]

32. Individuals affected by surveillance or data-sharing practices often face barriers to access to effective remedies.[60] The extraterritorial nature of intelligence cooperation, the invocation of secrecy in the name of national security and the absence of notification requirements may hinder individuals from knowing that their data have been collected or shared, or from challenging the lawfulness of such measures.[61]

[49] A/HRC/39/29, paras. 21 and 22; A/HRC/40/63, para. 36; OHCHR, *Fact Sheet No. 32*, pp. 54 and 55; and Privacy International, Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards (London, 2018), pp. 11, 19 and 23.

[50] A/HRC/10/3, para. 48; and Huszti-Orbán and Ní Aoláin, "Use of biometric data to identify terrorists", pp. 28 and 29.

[51] OHCHR, *Fact Sheet No. 32*, pp. 54–56; and A/HRC/14/46, para. 47.

[52] A/79/324, paras. 26 and 44; and A/HRC/39/29, para. 21.

[53] A/HRC/27/37, paras. 19, 26 and 27.

[54] A/HRC/40/63, para. 36; and Human Rights Council resolution 54/21, para. 10 (d).

[55] A/HRC/10/3, para. 48; A/HRC/27/37, paras. 30 and 33; and A/HRC/40/63, para. 36.

[56] Privacy International, Secret Global Surveillance Networks, pp. 11, 12, 19 and 23.

[57] Huszti-Orbán and Ní Aoláin, "Use of biometric data to identify terrorists", p. 28.

[58] United Nations Convention against Cybercrime, art. 28 (4).

[59] OHCHR, "UN experts: safeguard human freedoms"; A/HRC/39/29, para. 22; and OHCHR, *Fact Sheet No. 32*, p. 52.

[60] A/HRC/27/37, paras. 39–41; and A/HRC/39/29, para. 22.

[61] A/HRC/27/37, para. 40; and OHCHR, *Fact Sheet No. 32*, pp. 54 and 55.

Advance edited version

IV. Update on the human rights implications of counter-terrorism practices

33. Human rights challenges do not arise from data- or technology-driven counter-terrorism measures alone, but reflect broader structural shortcomings in counter-terrorism practices, which data and digital approaches may further exacerbate.

34. During the reporting period, terrorism continued to have devastating consequences for individuals, communities and societies, including through loss of life, physical injury, psychological trauma, displacement and disruption of livelihoods. States have a responsibility to protect persons within their territory and subject to their jurisdiction from acts of terrorism, in accordance with international law. At the same time, OHCHR, United Nations human rights mechanisms and civil society documented a range of human rights implications of counter-terrorism practices. Vague legal definitions of terrorism and insufficient safeguards have led to violations and abuses of human rights with disproportionate consequences for already vulnerable groups. An update on recent developments is provided in the present section.

35. Certain counter-terrorism measures have been found to have a chilling effect on civil society, discouraging individuals and communities from participating in public life and narrowing the space for freedom of expression, association and peaceful assembly.[62] Beyond the chilling effect of surveillance discussed in the previous section, vague and overbroad terrorism definitions have at times been applied to silence individuals peacefully exercising their fundamental freedoms, including journalists, political opponents and human rights defenders.[63] In several settings, this has led to the harassment, surveillance or criminalization of journalists, human rights defenders and civil society organizations.[64] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted that, in the Philippines, "red-tagging" – the practice of vilification and harassment consisting in the labelling of activists and reporters as terrorists – had been associated with unlawful surveillance, arbitrary detention and, in some cases, killings.[65] In Algeria, terrorism-related charges reportedly continued to be brought against individuals peacefully exercising their fundamental freedoms, including trade unionists, journalists and human rights defenders, amid concerns that legislative amendments introduced in 2024 to broaden the scope of terrorism-related offences may facilitate the suppression of dissent.[66] In relation to Saudi Arabia, the Committee on the Elimination of Racial Discrimination and the Committee on the Elimination of Discrimination against Women expressed concern about reports of the use of counter-terrorist and anti-cybercrime legislation to target human rights defenders and activists, including women's rights advocates, resulting in intimidation, arbitrary arrest, harassment and detention.[67]

36. Similar misuse of counter-terrorism and extremism laws has been reported in relation to Belarus, Iran (Islamic Republic of), Myanmar, the Russian Federation and Türkiye, where journalists, lawyers, political opponents, civic activists and human rights defenders have been prosecuted or detained on terrorism-related charges.[68] The Human Rights Committee has

[62] OHCHR, "UN experts: safeguard human freedoms"; A/HRC/61/52, para. 5; and OHCHR, *Fact Sheet No. 32*, pp. 29 and 30.

[63] A/HRC/61/52, para. 5.

[64] A/HRC/40/52 (2019), paras. 8 and 43. See also submissions from CIVICUS – World Alliance for Citizen Participation and MENA Rights Group.

[65] A/HRC/59/50/Add.1, paras. 21–27.

[66] See submission from CIVICUS – World Alliance for Citizen Participation.

[67] CERD/C/SAU/CO/10-11, paras. 27 and 28; and CEDAW/C/SAU/CO/5, para. 17. See, as an example, the case of Manahel al-Otaibi: submission from MENA Rights Group, pp. 16 and 17; and SAU 4/2024 (all communications mentioned in the present document are available from https://spcommreports.ohchr.org/Tmsearch/TMDocuments).

[68] On Belarus, see OHCHR, "Belarus must end ill-treatment of prisoners convicted on terrorism and extremism charges, say UN experts", 15 August 2025; and OHCHR, "UN experts urge Belarus to stop interfering in the legal profession", 17 November 2025. On the Islamic Republic of Iran, see OHCHR, "Iran: UN Human Rights Chief urges authorities to end violent repression and calls for

Advance edited version

expressed concern about the misuse of counter-terrorism legislation to target civil society organizations in Türkiye[69] and about the disproportionate impact of the application of broadly defined terrorism offences on human rights defenders, journalists, dissidents and members of ethnic and religious minorities in Pakistan.[70]

37. In July 2025, the Government of the United Kingdom of Great Britain and Northern Ireland proscribed Palestine Action as a terrorist organization under the Terrorism Act 2000. The decision prompted concerns regarding the application of counter-terrorism legislation in relation to acts that, while criminal, might not meet the threshold of "terrorism" under international standards,[71] and the impact of such application on the rights to freedom of expression, peaceful assembly and association. Further concerns were raised about the subsequent use of the proscription to arrest and detain individuals accused of supporting or identifying with Palestine Action, including through signs, clothing or participation in peaceful demonstrations, on terrorism-related charges.[72] Those concerns persisted following the decision of the Court of Appeal in June 2025 to uphold the proscription,[73] and it remains unclear whether the Supreme Court will hear an appeal.[74]

38. In West Africa, information gathered by OHCHR indicated that counter-terrorism frameworks, adopted in response to genuine security threats, had been applied in ways that raised serious human rights concerns. In Benin, concerns were raised over the overbroad and at times arbitrary application of counter-terrorism legislation against human rights defenders, journalists, civil society actors and political opponents, leading to arbitrary arrests and a contraction of civic space, as well as the stigmatization of Fulani and herder communities. In Côte d'Ivoire, the 2015 anti-terrorism law was reportedly used to charge opposition members with "terrorist acts" ahead of the 2025 presidential elections, raising concerns about its use to restrict democratic participation. In Togo, a state of security emergency in Savanes Region was extended until March 2027, with civil society organizations denied access to the affected area and reports of multiple cases of arbitrary arrest and enforced disappearance.

39. Counter-terrorism laws have also generated a broader chilling effect on civil society, particularly humanitarian and human rights organizations operating in conflict-affected contexts. The establishment by the United States Department of Justice in March 2025 of "Joint Task Force October 7", mandated to investigate acts of terrorism by individuals and entities providing support and financing to Hamas, raised concerns that its broad mandate – encompassing both financial crime and counter-terrorism – could result in heightened scrutiny of humanitarian, advocacy and human rights organizations working in relation to Palestine, with potential implications for freedom of expression and association and the ability to carry out humanitarian work.[75]

---

accountability", 13 January 2026; A/HRC/61/59, paras. 29 and 30; and the conference room paper containing the consolidated findings of the Independent International Fact-Finding Mission on the Islamic Republic of Iran, available at https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session61/list-reports. On Myanmar, see OTH 82/2025. On the Russian Federation, see OHCHR, "Russia's repression policy to dismantle civil society exposes fear of accountability: UN Special Rapporteur", 11 December 2025; OHCHR, "Strategy of blatant abuse of counter-terrorism and extremism laws to destroy Russian civil society must end: UN experts", 9 April 2026; and Amnesty International, "Russia: surge in abuse of anti-terrorism laws to suppress dissent", 19 February 2024. On Türkiye, see OHCHR, "Türkiye: expert dismayed by continued misuse of counter-terrorism law to keep human rights defenders in long-term detention", 16 January 2025.

[69] CCPR/C/TUR/CO/2, para. 17.

[70] CCPR/C/PAK/CO/2, para. 26.

[71] OHCHR, "UK: Palestine Action ban 'disturbing misuse' of UK counter-terrorism legislation, Türk warns", 25 July 2025; and OHCHR "UN experts urge United Kingdom not to misuse terrorism laws against protest group Palestine Action", 1 July 2025.

[72] See GBR 13/2025; and OHCHR, "UK: Palestine Action ban".

[73] England and Wales, Court of Appeal (Civil Division), *Secretary of State for the Home Department v. Ammori*, Judgment, 15 June 2026.

[74] Dominic Casciani and Amy Walker, "Palestine Action ban is lawful, Court of Appeal rules", British Broadcasting Corporation, 15 June 2026.

[75] See submission from Charity and Security Network; and Charity and Security Network, "Shadow report submission to Financial Action Task Force (FATF): U.S. FATF Mutual Evaluation 2026", December 2025, p. 12 and 13.

Advance edited version

40. The expanding application of counter-terrorism frameworks extends beyond civil society organizations to encompass other actors and activities traditionally outside their scope.[76] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism cautioned against the use of counter-terrorism laws in combating organized crime associated with drug trafficking, under the label "narco-terrorism", to justify exceptional legal powers, including investigative and intelligence powers, administrative restrictions and arbitrary detention.[77] Between September 2025 and June 2026, military strikes carried out by the United States against vessels in the Caribbean and eastern Pacific, framed as targeting "narco-terrorists", killed at least 210 individuals.[78] The High Commissioner noted that those strikes were incompatible with international law.[79]

41. El Salvador and Honduras have designated organized criminal groups, including drug trafficking organizations and gangs, as terrorist entities. In Argentina and Ecuador, such designations have justified exceptional security measures, including prolonged states of emergency and the use of force in ways that fall short of human rights standards.[80] These practices have expanded the scope of counter-terrorism powers beyond their original purpose, with consequences for due process guarantees, judicial oversight and the rights of the populations affected.

42. Counter-terrorism frameworks have also been applied in a manner that undermines due process guarantees and fair trial rights.[81] For example, the Committee against Torture expressed concern about reports that persons detained for terrorism-related offences in Bahrain were not routinely afforded all fundamental legal safeguards from the very outset of deprivation of liberty, including prompt access to legal counsel and judicial review.[82] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism noted that, in Benin, many terrorism suspects had been held in protracted pretrial detention for two to three years and some for as long as five years, and that the duration of terrorism cases contrasted with the disposal of other cases within very short periods, potentially indicating insufficient prioritization of expeditious terrorism trials.[83] Similarly, in India, activists and human rights defenders had been kept in pretrial detention for over four years without an individualized determination of the reasonableness and necessity of the detention.[84] In Pakistan, in August 2025, the National Assembly passed amendments to the Anti-Terrorism Act, 1997, authorizing the detention for inquiry, for up to three months, of individuals suspected of involvement in terrorism-related offences based merely on credible information or reasonable suspicion, without judicial oversight.[85] In

[76] OHCHR, *Fact Sheet No. 32*, pp. 21 and 22.

[77] See the remarks of the Special Rapporteur at the side event on "The abuse of counter-terrorism law to combat drugs and other organized crime", held on 11 March 2006 during the sixty-first session of the Human Rights Council, available at https://www.ohchr.org/en/special-procedures/sr-terrorism/activities.

[78] See Konstantin Toropin, "US strike on an alleged drug boat kills 2, leaves 6 survivors, in the Caribbean", Associated Press, 22 June 2026; and Heather Mongilio, "Two men killed in U.S. strike on suspected drug boat in the Caribbean", United States Naval Institute News, 22 June 2026.

[79] OHCHR, "US attacks in Caribbean and Pacific violate international human rights law – UN Human Rights Chief", 31 October 2025.

[80] See submission from Centro de Estudios Legales y Sociales, Asociación Civil (CELS) (in Spanish); and submission from International Drug Policy Consortium.

[81] Human Rights Committee, general comment No. 32 (2007), paras. 22 and 23; and OHCHR, *Fact Sheet No. 32*, pp. 47–49.

[82] CAT/C/BHR/CO/4, para. 15.

[83] A/HRC/58/47/Add.1, para. 29.

[84] For example, A/HRC/WGAD/2025/66, paras. 73–77. See also Amnesty International, "India: free Umar Khalid – stop invoking counter-terrorism law to silence dissent", 12 September 2025; and OHCHR, "UN experts alarmed by Indian counter-terrorism operations violating human rights in Jammu and Kashmir", 24 November 2025.

[85] See submission from CIVICUS – World Alliance for Citizen Participation; and PAK 12/2025.

Advance edited version

Viet Nam, special procedure mandate holders reported that individuals charged with vague and overbroad terrorism offences had been prosecuted in a mass trial by a "mobile court", which did not guarantee international fair trial rights.[86]

43. Fair trial guarantees have also been undermined in the context of counter-terrorism proceedings. OHCHR observed that, in Tunisia, proceedings in a number of cases related to counter-terrorism appeared not to comply fully with fair trial guarantees, including through the routine reliance since March 2025 on hearings held by videoconference, without individualized assessments of necessity, which limited defendants' ability to appear in person and adequately prepare their defence. In Myanmar, special procedure mandate holders reported that terrorism-related cases were tried by military courts or special courts controlled by the military, which lacked independence, in proceedings held behind closed doors with inadequate legal representation and characterized by other serious violations of fair trial guarantees.[87]

44. The human costs of these due process failures and of counter-terrorism measures more broadly are not evenly distributed. Certain groups, such as persons with disabilities, face compounded and disproportionate risks. OHCHR observed that hearings held by videoconference in counter-terrorism proceedings in Tunisia, for example, did not take into consideration specific vulnerabilities, including those of persons with sensory or hearing impairments. In relation to Ukraine, the Committee on the Rights of Persons with Disabilities expressed concern about the processing, under martial law, of sensitive and high-risk data related to the fight against terrorism, and about the absence of comprehensive provisions on the protection of personal data and records of persons with disabilities.[88]

45. Children are particularly vulnerable to the adverse effects of counter-terrorism measures. In relation to Israel, the Committee against Torture expressed concern over the passing, in 2024, of Amendment No. 25 (on temporary provisions) to the Youth Law (Trial, Punishment and Treatment Methods), which lowered the age for imprisonment to 12 years if a child was convicted of an act of terror.[89] The Committee on the Rights of the Child urged Israel to repeal that amendment.[90]

46. Ethnic and religious minorities and migrants are similarly disproportionately targeted. In relation to Türkiye, the Committee on the Protection of the Rights of All Migrant Workers and Members of Their Families expressed concern about the lack of information on the detention of migrant workers and members of their families; on the practices employed in relation to migration detention; and with regard to detention linked to security reasons, such as of those designated as foreign terrorist fighters.[91] In relation to the United Kingdom, the Committee on the Elimination of Racial Discrimination expressed concern about the high number of interventions and referrals of persons belonging to Muslim communities, in particular children, to the "Prevent" counter-terrorism programme.[92] In relation to Kenya, the same Committee expressed concern about reports of arbitrary arrest and detention, extortion, forced relocation and other abuses committed by State officials in the context of counter-terrorism operations, and about reports that counter-terrorism measures had created an atmosphere of suspicion and marginalization towards ethno-religious minorities, particularly Muslim communities.[93] In relation to Viet Nam, the Human Rights Committee expressed concern about the application of national security and counter-terrorism laws to target religious minorities.[94] In relation to China, the High Commissioner raised concerns about counter-terrorism and assimilation policies, particularly as they affected minorities in

[86] See OHCHR, "Experts condemn misuse of counter-terrorism law against Montagnards in Viet Nam", 28 August 2024.
[87] OTH 82/2025, pp. 4 and 12.
[88] CRPD/C/UKR/CO/2-3, para. 44.
[89] CAT/C/ISR/CO/6, para. 22.
[90] CRC/C/ISR/CO/5-6, para. 49 (b).
[91] CMW/C/TUR/CO/2, para. 35 (b).
[92] CERD/C/GBR/CO/24-26, para. 33.
[93] CERD/C/KEN/CO/8-9, para. 27.
[94] CCPR/C/VNM/CO/4, para. 44.

Advance edited version

Xinjiang Uighur Autonomous Region, Inner Mongolia Autonomous Region and Tibet Autonomous Region, and called for the repeal of the law on ethnic unity, which could further restrict minority rights.[95]

47. The use of biometric technologies can lead to discriminatory profiling, disproportionately affecting minorities and other marginalized groups. [96] Biometric recognition systems have further been used to identify and track peaceful protesters and dissidents, raising concerns about discrimination on the basis of political opinion.[97] These developments illustrate how privacy-intrusive counter-terrorism measures may reinforce existing patterns of discrimination and exclusion, with consequences extending well beyond the right to privacy.

V. Conclusions and recommendations

A. Conclusions

48. **The right to privacy remains acutely exposed to the expansion of data-driven and technology-enabled counter-terrorism measures. Data-driven and technology-enabled security practices, including digital surveillance, biometric identification and algorithmic risk assessment, now play a central role in the implementation of counter-terrorism measures, significantly expanding States' capacity to collect, process and share personal data. While such tools may contribute to legitimate security objectives, their growing use has raised concerns regarding their impact on the right to privacy, particularly where they are deployed under broadly defined national security mandates, in the absence of a genuine security threat, through administrative procedures and in the absence of sufficient and adequate safeguards.**

49. **In the absence of adequate legal frameworks and safeguards, these practices pose serious risks of undue interference with the right to privacy, interference that in turn enables and compounds restrictions on other fundamental rights, including freedom of expression and association. These practices may also have a negative impact on fair trial guarantees. Persistent oversight and accountability gaps remain, as the use of technologies in counter-terrorism contexts and practices has expanded faster than the frameworks designed to regulate them. Surveillance systems, administrative measures and cross-border intelligence cooperation frequently entail a lack of sufficient transparency, oversight and access to effective remedies. In many contexts, counter-terrorism measures that were initially conceived as exceptional and time-restricted have become permanent features of States' security architecture. In the absence of stronger compliance with international human rights law, this structural shift threatens both the right to privacy and the broader rule of law.**

B. Recommendations

50. **The High Commissioner recommends that States:**

(a) **Ensure that the right to privacy, as protected under article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, is central to the design and implementation of**

[95] OHCHR, "Türk says ultimate trajectory for human rights is larger freedom", 16 June 2026, available at https://www.ohchr.org/en/statements-and-speeches/2026/06/turk-says-ultimate-trajectory-human-rights-larger-freedom. See also OHCHR, "China: update on the work of UN Human Rights Office", 27 August 2024; and UN News, "China: UN rights office reiterates need to review national security framework", 27 August 2024.

[96] Huszti-Orbán and Ní Aoláin, "Use of biometric data to identify terrorists", pp. 24, 25 and 27; Counter-Terrorism Committee Executive Directorate, "CTED analytical brief", p. 5; A/HRC/60/45, para. 19; and Committee on the Elimination of Racial Discrimination, general recommendation No. 36 (2020), para. 35.

[97] A/HRC/60/45, para. 19.

Advance edited version

counter-terrorism frameworks, and that any interference with this right is lawful, necessary and proportionate to the pursuit of a legitimate aim and does not impair the essence of that right;

(b) **Review counter-terrorism legislation to ensure that terrorism-related offences and powers are clearly defined and comply with the principles of legality and legal certainty, and that broad or vague definitions are not used to target human rights defenders, journalists, civil society organizations or minority and marginalized communities;**

(c) **Ensure that any interference with the right to privacy in counter-terrorism contexts is prescribed by law, limited in scope and duration and subject to prior authorization and ongoing supervision by an independent and impartial authority, ordinarily a judicial one;**

(d) **Refrain from the use of mass or indiscriminate surveillance measures under counter-terrorism strategies and policies and ensure that technologies introduced for specific security purposes are used for broader population monitoring;**

(e) **Subject the design, procurement and deployment of high-risk technologies, including biometric identification systems and artificial intelligence, in counter-terrorism contexts to mandatory systematic human rights impact assessments, throughout their life cycle, that take into account the broader legal and technological environment in which such systems operate, with particular attention to the risks of discriminatory profiling and cumulative effects on minorities, migrants, children and marginalized groups, and ensure that automated decision-making is subject to meaningful human review;**

(f) **Regulate the involvement of private actors in counter-terrorism activities through clear legal frameworks requiring human rights due diligence, transparency and accountability;**

(g) **Strengthen independent oversight and accountability mechanisms with the authority, technical expertise and access to classified information necessary to review counter-terrorism measures effectively, including measures involving surveillance technologies, intelligence cooperation and private sector participation, and ensure sufficient transparency, including through public reporting, to enable meaningful oversight;**

(h) **Guarantee access to effective remedies for individuals affected by counter-terrorism measures, including timely notification of surveillance measures subject only to strictly necessary limitations, access to reasons and evidence, and the ability to challenge decisions before an independent body;**

(i) **Strengthen international counter-terrorism cooperation in a manner consistent with international human rights law, including by ensuring that data-collection and data-sharing arrangements are grounded in law and subject to data-protection safeguards, protect against misuse and onward transfer and exclude reliance on information obtained through unlawful means, torture or other ill-treatment;**

(j) **Ensure that measures addressing linkages between terrorism and organized crime are assessed on a case-by-case basis and grounded in context-specific analysis of actors' motivations and local dynamics, and that any designation of an organized criminal group as a terrorist entity is based on clear and precise legal criteria, complies with the principles of legality, necessity and proportionality and is subject to regular independent review.**

51. **The High Commissioner recommends that United Nations entities:**

(a) **In providing technical assistance and capacity-building to States on counter-terrorism, fully integrate human rights due diligence into project design and operations, and condition assistance on the existence of adequate legal frameworks and independent oversight mechanisms for any surveillance, biometric or data-processing tools involved, in accordance with human rights due diligence policy as set out in**

Advance edited version

relevant United Nations frameworks and guidance, including the guidance of the Secretary-General on human rights due diligence for digital technology use;

(b) **Within the scope of their mandates, provide technical guidance and support to States to establish independent oversight mechanisms for counter-terrorism measures, including measures involving surveillance technologies, artificial intelligence, biometric systems and cross-border data-sharing arrangements, and assess and address the impact of such measures on the human rights of the individuals and communities affected, including minorities, migrants and other marginalized groups;**

(c) **Integrate international human rights standards into the development or dissemination of guidance on the use of artificial intelligence, biometric technologies and other data-driven tools in counter-terrorism.**

Advance edited version