UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

INTERPOL

Funded by
the European Union

Cybersecurity and New Technologies

Guide for Human-Rights Based Approach to Countering Use of New Technologies for Terrorist Purposes

---

Acknowledgements

This report is the product of a joint initiative between the United Nations Counter-Terrorism Centre (UNCCT) of the United Nations Office of Counter-Terrorism (UNOCT) and INTERPOL on strengthening capacities of law enforcement and criminal justice authorities to counter the use of new technologies for terrorism purposes. The joint initiative was funded with generous contributions from the European Union.

Contents

Joint Foreword

Advances in Information and Communication Technologies (ICT) and their availability have made it attractive for terrorist and violent extremist groups to exploit them to facilitate a wide range of activities, including incitement, radicalization, recruitment, training, planning, collection of information, communication, preparation, propaganda, and financing. Terrorists continuously explore new technological frontiers, and Member States have been expressing increasing concerns over the use of new technologies for terrorist purposes.

During the seventh review of the United Nations Global Counter-Terrorism Strategy, Member States requested the United Nations Office of Counter-Terrorism and other relevant Global Counter-Terrorism Co-ordination Compact entities to "jointly support innovative measures and approaches to building the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism".

In his report to the General Assembly on the Activities of the United Nations system in implementing the United Nations Global Counter-Terrorism Strategy (A/77/718), the Secretary-General underscores that "[...] new and emerging technology offers unmatched opportunities to improve human welfare and new tools to counter-terrorism. [...] Despite strengthened and concerted efforts, responses by the international community often lag behind. Some of these responses unduly limit human rights, in particular the rights to privacy and to freedom of expression, including to seek and receive information".

Through the seven reports contained in this compendium – the product of the partnership between the United Nations Counter-Terrorism Centre and the International Criminal Police Organization under the CT TECH joint initiative, funded by the European Union – we seek to support Member States' law enforcement and criminal justice authorities to counter the exploitation of new and emerging technologies for terrorist purposes and to leverage new and emerging technologies in the fight against terrorism as part of this effort, in full respect of human rights and the rule of law.

Our Offices stand ready to continue to support Member States and other partners to prevent and counter-terrorism in all its forms and manifestations and to take advantage of the positive effects of technology in countering terrorism.

Vladimir Voronkov
Under-Secretary-General, United Nations Office of Counter-Terrorism
Executive Director, United Nations Counter-Terrorism Centre

Stephen Kavanagh
Executive Director,
Police Services INTERPOL

Acknowledgements

This document has been developed through the contributions and reviewed by a wide range of stakeholders. Specifically, the United Nations Office of Counter-Terrorism (UNOCT) wish to acknowledge the contribution made by the following:

- **Mr. Kamel El Hilali** – PhD in Law
  Paris Pantheon Assas University;
- **Mr. Paul Madden** – Project Lead Counter-TerrorismPHARE,
  The International Institute for Justice and the Rule of Law (IIJ);
- **Mr. Tomaso Falchetta** – Head of Advocacy and Policy
  Privacy International;
- **Mr. Tom Parker** – Project Coordinator, Terrorism Prevention Branch
  United Nations Office on Drugs and Crime (UNODC); and
- **Mr. Victor Kipkoech** – Programme Associate
  Global Center on Cooperative Security (GCCS)

Terms and Definitions

Artificial Intelligence	Generally understood to describe a discipline concerned with developing technological tools exercising human qualities, such as planning, learning, reasoning, and analising.
Criminal Justice Process	A legal process to bring about criminal charges against an individual or an entity and the court proceedings, judgement sentencing as well as corrections and rehabilitation.
Darknet/ Dark Web	The encrypted part of the Internet accessed using specific software that in themselves are not criminal, such as the Tor browser. However, it is recognized that the dark web contains many criminal websites and services which are hosted on these networks.[1]
Disengagement	The process in which someone who shows signs of having been radicalized is coached into either "leav[ing] their group or reject[ing] violence, while not necessarily aiming to change their underlying extremist viewpoints or ideology."[2]
Evidence	A formal term for information that forms part of a trial in the sense that it is used to prove or disprove the alleged crime. All evidence is information, but not all information is evidence. Information is thus the original, raw form of evidence.[3]

1 European Cybercrime Center (EC3), Internet Organized Crime Threat Assessment 2019 (Europol, 2019), https://www.europol.europa.eu/cms/sites/default/files/documents/iocta_2019.pdf

2 Ibid, page 8.

3 CTED Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences (2019), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_military_evidence_guidelines.pdf

Incitement to Terrorism	Intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.
Intelligence	The product resulting from collecting, developing, disseminating, analising, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law.
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support the prosecution in legal proceedings.
Law Enforcement Actions	Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e. content removal, asset seizures), etc.
New Technologies	While the new technologies terminology covers a wide range of different technologies[4], for the purpose of this document new technologies refer to the use and abuse of such new technologies as the Internet, social media, cryptocurrencies, facial recognition and darknet.[5]
Rehabilitation	In a criminal justice context, the term 'rehabilitation' is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the offender's reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.
Terrorism	Criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism.[6]
Virtual assets	Virtual/crypto assets refer to digital forms of currency and other assets.[7]
VLOPs	Very large Online Platforms and Search Engines.
Zettabyte	One zettabyte is equal to one billon terabytes.

4 Artificial Intelligence, Internet of things, block chain technologies, crypto-assets, drones and unmanned aerial systems, DNA, fingerprints, cyber technology, facial recognition, 3D printing.

5 CT TECH Project Document – Annex I Description of the Action

6 See S/RES/1566 (2004), para. 3. For more information, see Section 5.1.

7 Financial Action Task Force (FATF), "Virtual Assets," Financial Action Tast Force (FATF), accessed May 7, 2023, https://www.fatf-gafi.org/en/topics/virtual-assets.html

Executive Summary

International human rights law imposes on Member States a positive obligation to take appropriate steps to protect persons within their jurisdiction from a host of threats to their security including the threat of terrorism. Formulating appropriate responses to terrorism has grown steadily more complex as terrorist actors have increasingly exploited a range of new technologies to support, prepare, and conduct terrorist acts, as well as to spread disinformation, incite to violence and recruit new members. Indeed, some Member States have taken a range of measures at odds with international human rights law, including, inter alia: grounded in insufficiently clear or overbroad definitions of terrorism, taking criminal justice measures against individuals or groups such as civil society actors, human rights defenders, journalists or the political opposition for exercising their human rights, including their freedom of expression online; engaging in unlawful or arbitrary online surveillance; unduly restricting access to services or content such as through Internet shutdowns, throttling or blocking of websites. Given the harms to a broad range of human rights and the rule of law resulting from such measures, the risk is real that such counter-terrorism efforts conducted in contravention of international law may lead to the misapplication or inefficient use of resources, and in fact exacerbate existing grievances and contribute to conditions conducive to radicalization to violence.

This report on human-rights based approaches to countering the use of new technologies for terrorist purposes aims to assist policy makers and those implementing those policies to ensure that counter-terrorism responses are provided by law, pursue a legitimate aim, and necessary and proportionate to the threat at issue in order that they do not violate individuals' human rights and/or reinforce existing grievances.

[1]

Background

1.1 Overview

United Nations Member States attach great importance to addressing the impact of new technologies in countering terrorism. During the seventh review of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[8] in July 2021, Member States expressed their deep concern about "*the use of the Internet and other information and communications technologies, including social media platforms, for terrorist purposes, including the continued spread of terrorist content,*" and requested the Office of Counter-Terrorism and other Global Counter-Terrorism Compact entities "*to jointly support innovative measures and approaches to build the capacity of Member States, upon their request, for the challenges and opportunities that new technologies provide, including the human rights aspects, in preventing and countering terrorism*". Security Council resolutions 2178 (2014)[9] and 2396 (2017)[10] call for Member States to act cooperatively when taking national measures to prevent terrorists from exploiting technology and communications for terrorist acts. Security Council Resolution 2396 (2017) also encourages Member States **to enhance cooperation with the private sector, especially with ICT companies,**, in gathering digital data and evidence in cases related to terrorism.

In its 30th Report to the United Nations Security Council[11], the Analytical Support and Sanctions Monitoring Team noted that "*Many Member States highlighted the evolving role of social media and other online technologies in the financing of terrorism and dissemination of propaganda*", with platforms cited by Member States include Telegram, Rocket. Chat, Hoop and TamTam, among others. **ISIL (Da'esh) supporters using platforms on the dark web** for storing and accessing training materials that other sites decline to host as well as **for acquiring new technologies** were also cited in the report.

Countering the use of new and emerging technologies for terrorists' purposes was discussed at the dedicated special meeting of the United Nations Security Council's Counter-Terrorism Committee's (CTC), which took place on 28-29th October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration[12].

8 The United Nations Global Counter-Terrorism Strategy: seventh review (A/RES/75/291), N2117570.pdf (un.org)

9 Security Resolution 2178 (2014), S/RES/2178%20(2014)(undocs.org)

10 Security Resolution 2396 (2017), http://undocs.org/S/RES/2396(2017)

11 Thirtieth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2610 (2021) concerning ISIS (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities S/2022/547 (undocs.org)

12 The Delhi Declaration, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_special_meeting_outcome_document.pdf

The CTC noted "***with concern the increased use, in a globalized society, by terrorists and their supporters of the Internet and other information and communication technologies***, *including social media platforms, for terrorist purposes*" and acknowledged "***the need to balance fostering innovation and preventing and countering the use of new and emerging technologies, as their application expands, for terrorist purposes***", while emphasizing "***the need to preserve global connectivity and the free and secure flow of information*** *facilitating economic development, communication, participation and access to information*".

1.2 CT TECH Initiative

CT TECH is a joint UNOCT/ UNCCT and INTERPOL initiative, implemented under the UNOCT/UNCCT Global Counter-Terrorism Programme on Cybersecurity and New Technologies. It is aimed at strengthening capacities of law enforcement and criminal justice authorities in selected Partner States to counter the exploitation of new and emerging technologies for terrorist purposes, as well as support Partner States' law enforcement agencies in leveraging new and emerging technologies in the fight against terrorism.

To achieve the overall objective, the CT TECH initiative implements two distinct outcomes with six underpinning outputs.

FIGURE 1

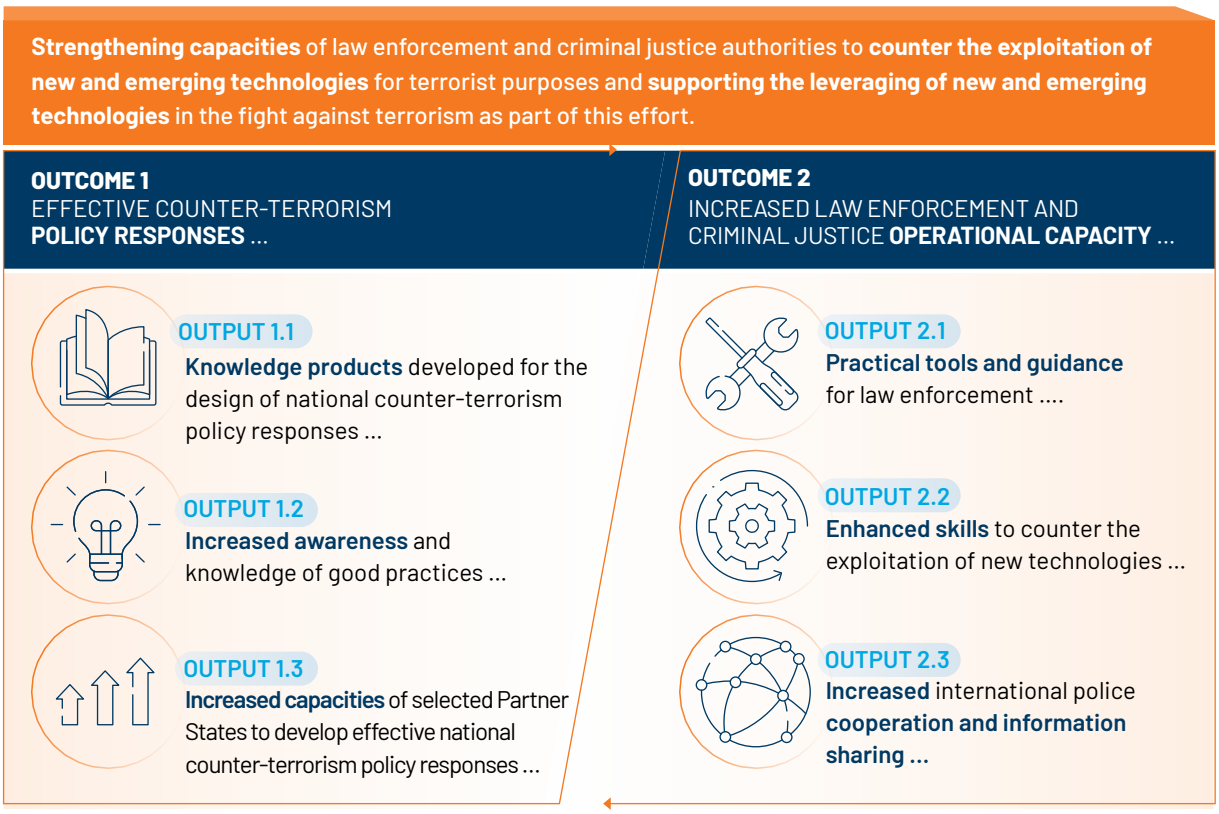


TABLE 1. **CT TECH Outcomes and Outputs**

Outcome 1: Effective counter-terrorism policy responses towards the challenges and opportunities of new technologies in countering terrorism in full respect of human rights and rule of law.	
Output 1.1	Knowledge products developed for the design of national counter-terrorism policy responses to address challenges and opportunities of new technologies in countering terrorism in full respect of human rights and the rule of law are developed.
Output 1.2	Increased awareness and knowledge of good practices on the identification of risks and benefits associated with new technologies and terrorism in full respect of human rights and the rule of law.
Output 1.3	Increased capacities of selected Partner States to develop effective national counter-terrorism policy responses towards countering terrorist use of new technologies and leveraging new technologies to counter-terrorism in full respect of human rights and the rule of law.
Outcome 2: Increased law enforcement and criminal justice operational capacity to counter the exploitation of new technologies for terrorist purposes and use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law.	
Output 2.1	Practical tools and guidance for law enforcement on countering the exploitation of new technologies for terrorist purposes and the use of new technologies to prevent and counter-terrorism in full respect of human rights and the rule of law is developed.
Output 2.2	Partner States' law enforcement and criminal justice institutions have enhanced skills to counter the exploitation of new technologies for terrorist purposes and use of new technologies to counter-terrorism in full respect of human rights and rule of law.
Output 2.3	Increased international police cooperation and information sharing on countering terrorist use of new technologies and using new technologies to counter-terrorism.

1.3 Document Purpose and Use

The purpose of this document is to assist policy makers and those implementing those policies ensuring that their responses are provided by law, justified in pursuit of a legitimate aim, necessary and proportionate to the threat at hand in order that they do not violate individuals' human rights and thus contravene obligations under international law and undermine the efficiency and sustainability of counter-terrorism efforts

1.3.1 Scope

The report addresses a range of new technologies including social media, the Internet more generally, facial recognition and algorithmic profiling, circumvention technologies, and spyware.

1.3.2 Target Audience

National security policy makers and senior officials responsible for executing those policies.

1.3.4 Limitations

With the exception of facial recognition and profiling technologies, this document does not address the benefits or risks associated with the use of artificial intelligence.

[II]

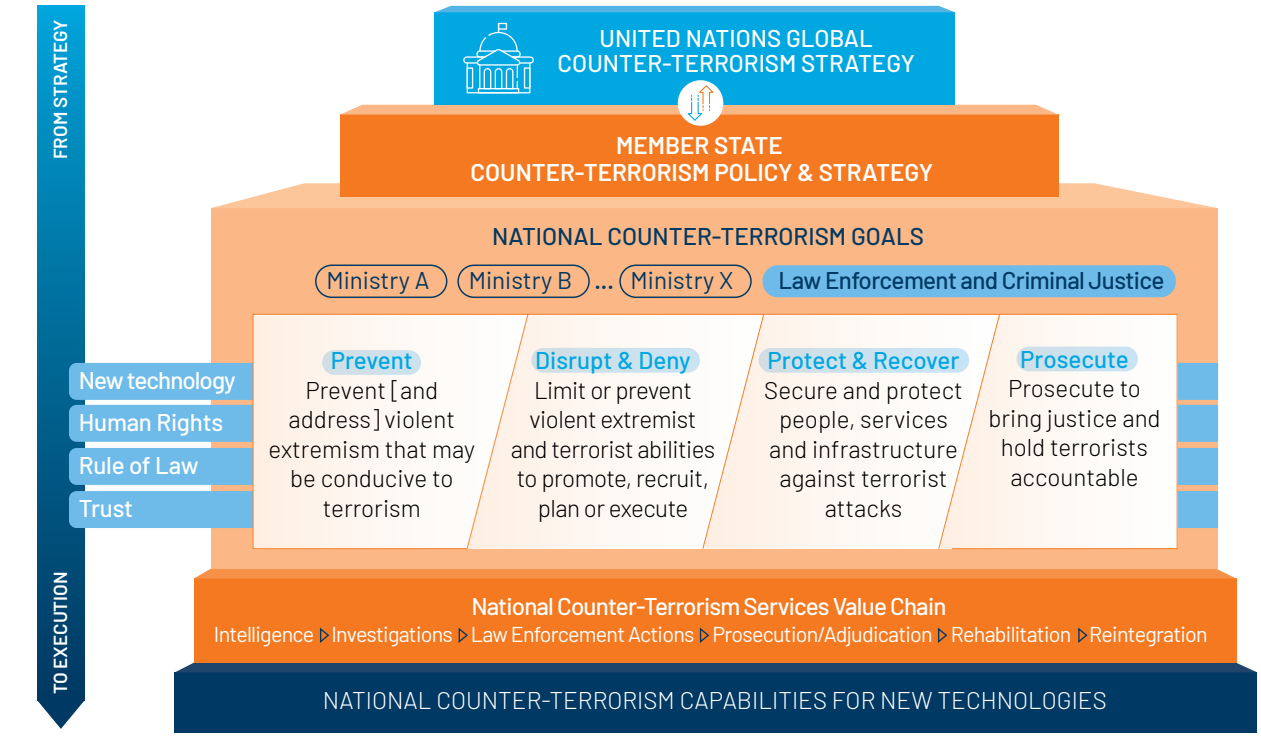
Approach

2.1 Overview

The report seeks to support and enable Member States to ensure and improve compliance with international human rights norms and standards and protection of civil liberties of individuals in countering the use of new technologies for terrorist purposes as well as employing technological tools to prevent and counter-terrorism., which are aligned to the United Nations Global Counter-Terrorism Strategy and in full respect of human rights and the rule of law.

2.2 Guiding Framework

FIGURE 2



The guiding framework is a conceptual model that is intended to guide, align, and inform the development of the report. It seeks to ensure coherence from strategy to execution between the United Nations Global Counter Terrorism Strategy (GCTS) and a Member State's National Counter-Terrorism Policy and Strategy goals and outcomes, services, and capabilities from a law enforcement and criminal justice perspective, regarding new technologies.

The United Nations GCTS, adopted by the General Assembly, sets out broad actions for Member States to address terrorism threat, which are set out across four key pillars:

Pillar I:	Measures to address the conditions conducive to the spread of terrorism
Pillar II:	Measures to prevent and combat terrorism
Pillar III:	Measures to build States' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in this regard
Pillar IV:	Measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism

Member States are encouraged to develop their respective national counter-terrorism legal and policy frameworks in alignment with the United Nations GCTS. They must ensure that their respective counter-terrorism laws, policies, strategies and measures comply with their obligations under international law, including international human rights law, international refugee law and international humanitarian law. A Member State's national counter-terrorism legal and policy framework should broadly seek to prevent and address violent extremism that may be conducive to terrorism, prevent or limit terrorist activities, take appropriate measures to protect persons within the State's jurisdiction, services and infrastructure against reasonably foreseeable threats of terrorist attacks, and ensure that terrorists are held accountable for their actions.

To achieve the counter-terrorism outcomes and goals, Member States' national law enforcement and criminal justice authorities have a set of tools at their disposal. These include, but are not limited to:

TABLE 2. **High-Level National Law Enforcement and Criminal Justice Services for Counter-Terrorism**

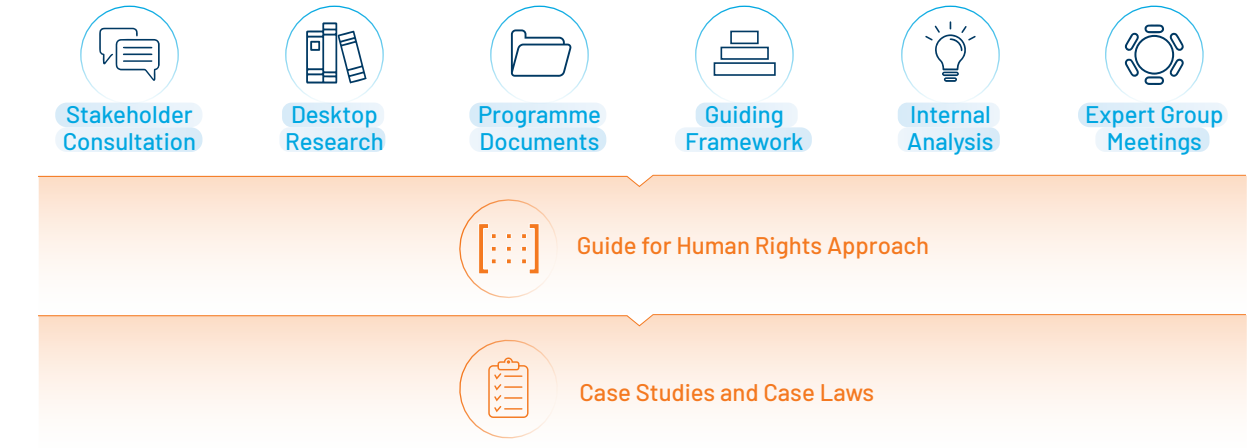
Services	Description
Criminal Justice Process	A legal process to bring about terrorism charges against an individual or an entity and the legal court hearing, ruling or judgement and sentencing as well as corrections and rehabilitation.
Intelligence	The product resulting from collecting, developing, disseminating, analising, and interpreting of information gathered from a wide range of sources, to inform decision makers for planning purposes to take decisions or actions – strategic, operational or tactical level. Intelligence should be collected, retained, used and shared in compliance with relevant Member State obligations under international human rights law.
Criminal Investigations	The process of collecting information (or evidence) to determine if a crime has been committed; identify the perpetrator and to provide evidence to support criminal justice proceedings.
Law Enforcement Actions	Typically describes law enforcement actions taken against a threat, which may include detaining individual(s), disrupting threat actor activities (i.e. content removal, asset seizures), etc.
Rehabilitation	In a criminal justice context, the term "'rehabilitation"' is used to refer to interventions managed by the corrections system with the aim to change the offender's views or behaviour to reduce the likelihood of re-offending and prepare and support the offender's reintegration back into society.
Reintegration	A comprehensive process of integrating a person back into a social and/or functional setting.

The effective use and deployment of such services and tools is dependent on a set of underlying capabilities. The required capabilities to enable and deliver services are often defined and represented in a capability model. A capability model represents a functional decomposition of key functions into a logical and granular grouping which supports the execution of services and activities. The capability model informs the requirements across people (structure and skills), processes, technology, infrastructure, and finance.

The guiding framework serves to ensure alignment between strategy and execution from both 'top-down' and 'bottom-up'.

2.3 Methodology

FIGURE 3



This document was developed and informed by a wide range of inputs which includes CT TECH project documents, stakeholder consultations, internal analysis, desktop research, Expert Group Meetings (EGM), co-ordination with the United Nations Global Counter-Terrorism Co-ordination Compact entities, and the guiding framework as described above in Section 2.2. From these activities, the key outputs of this document address salient human rights challenges and issues with regards to the development, deployment and use of new technologies, that may infringe on individuals' human rights. This analysis and is supported by a number of case studies.

2.3.1 Expert Group Meetings and Consultation

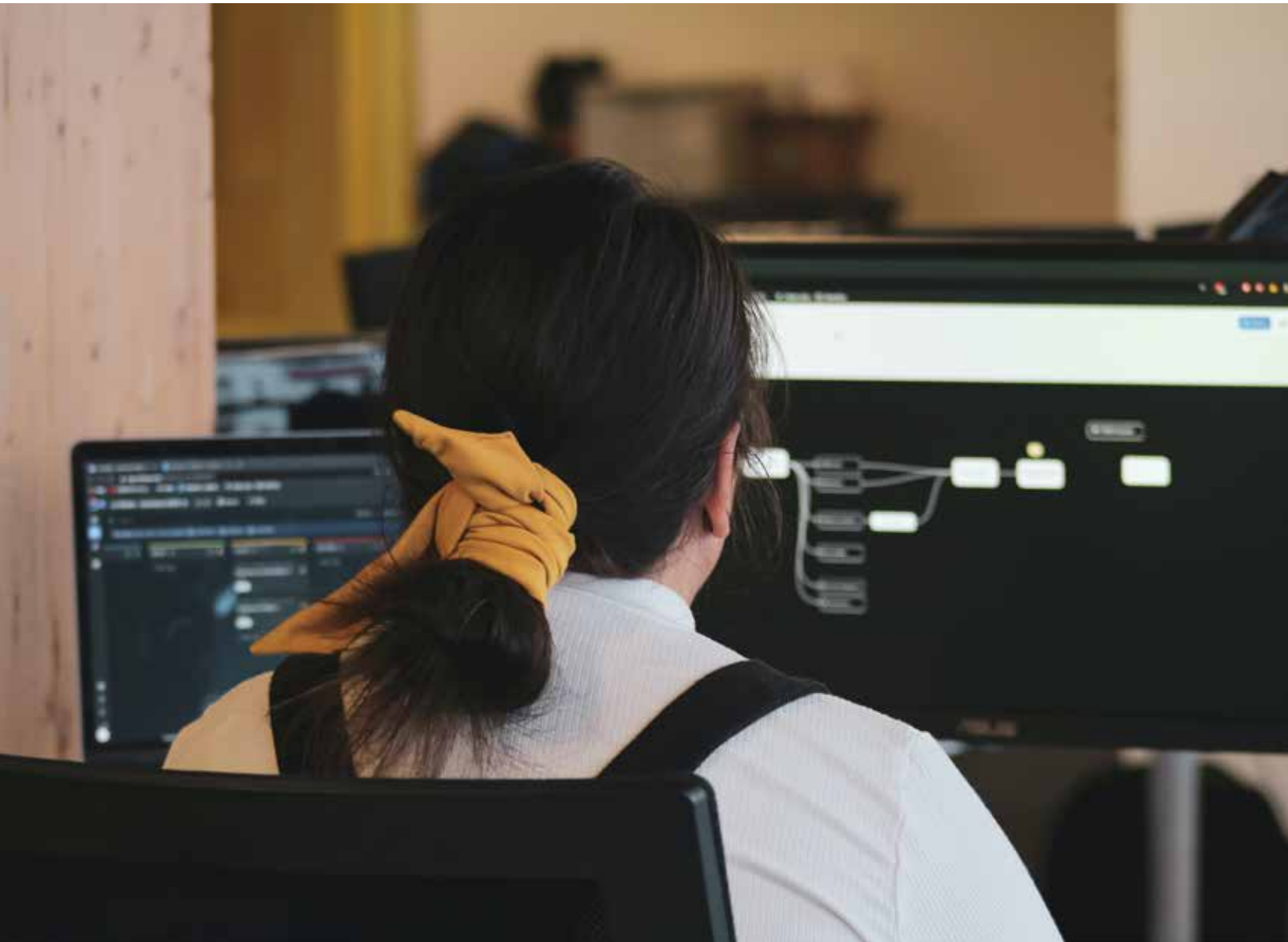
This guide has been developed with input by experts through the EGM sessions as well as individual consultations and review. The EGM brought together a group of experts and practitioners from counter-terrorism and law enforcement agencies (LEAs), human rights experts, private sector, academia and civil society to discuss how to counter use of new technologies for terrorist purposes and use new technologies as part of this effort, identify good practices in this regard, and also discuss risks, challenges and not so good practices that require attention and caution. The guide was further refined through engagement with the United Nations Global Counter-Terrorism Coordination Compact and its Working Group on Emerging Threats and Critical Infrastructure Protection, which promotes coordination and coherence to support the efforts of Member States to prevent and respond to emerging terrorist threats, in compliance with international human rights, international humanitarian and international refugee laws.

2.3.2 **Reference Document Review**

The development of this guide was informed by, took into consideration, built upon, and complemented existing research, guidelines and publications – which includes the following:

TABLE 3. **References**

1	The International Covenant on Civil and Political Rights
2	The International Convention on the Elimination of Racial Discrimination
3	Security Council Resolutions 1566 and 1624 and General Assembly Resolution 69/166
4	Case Law of the African Court of Human and Peoples' Rights; European Court of Human Rights and Court of Justice of the European Union; and Inter-American Court for Human Rights, as well as associated regional policy documents and statements
5	United Nations Global Counter-Terrorism Strategy
6	Reports of the Human Rights Council mandated Special Rapporteurs on the promotion and protection of human rights and fundamental freedoms while countering terrorism
7	Policy documents of the Office of the High Commissioner for Human Rights on privacy and new technologies



[III]

Introduction

3.1 Human Rights, Counter-Terrorism, and New Technologies

The development, widespread availability and use of a variety of new and emerging digital technologies have, in the past decades, rewired the way society functions. Access to and use of the Internet and ICTs has become essential to the conduct of government operations, to business, and individuals' day-to-day lives in many countries. In this respect, the United Nations Human Rights Council has recognized the promise these new and emerging technologies hold when it comes to facilitating efforts to accelerate human progress, enabling development, strengthening democratic institutions, empowering public participation and the open and free exchange of ideas. It has acknowledged the potential of such technologies to promote and protect human rights while also recognizing the risks that their abuse presents.[13]

> **"Member States must ensure that any measures taken to counter-terrorism comply with all their obligations under international law, in particular international human rights law, international refugee law and international humanitarian law [...] respect for human rights, fundamental freedoms and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are an essential part of a successful counter-terrorism effort."**
>
> United Nations Global Counter-Terrorism Strategy
> (General Assembly Resolution 75/291, Paragraph 9)

Indeed, the misuse of such technologies can give rise to serious security risks. We have witnessed in recent years examples of ways in which some technologies have been co-opted for criminal purposes and utilized among others to promote and support terrorist acts, by disseminating propaganda, online recruitment, radicalization and incitement to terrorism, for financing as well as for the execution of attacks. Mobile payment systems, online crowdfunding and virtual assets have been used by terrorist groups to circumvent financial controls. The same actors use social media and online gaming platforms to spread hate speech and terrorist content. Audio and video deep fakes can be used to challenge identity verification and fuel conspiracy.

13 A/HRC/RES/53/29

Cyber-attacks against critical infrastructure could disrupt vital societal functions and result in far-reaching impacts on a wide range of human rights, from the right to life and security of a person to the right to health and a healthy environment, the right to education, as well as water, sanitation and other aspects of the right to an adequate standard of living. 3-D printing and online technical instructions may ease terrorist access to weapons.[14]

At the same time, these same technologies facilitate the collection and preservation of information and evidence regarding terrorist activities; enable surveillance measures against suspected terrorists, their communications, their movements, and their finances. They facilitate the monitoring of weapons supplies and recruitment tactics, and they enable rapid dissemination of counter-terrorism narratives. However, Member States have at times faced challenges harnessing new technologies to counter-terrorism, including reducing terrorist exploitation of such technologies in a manner that fully complies with their obligations under international human rights law.[15]

The General Assembly and the Security Council have repeatedly emphasized that respect for human rights and the rule of law are complementary and mutually reinforcing with effective counter-terrorism measures, and are essential for successful and sustainable counter-terrorism efforts. Indeed, international human rights law imposes a due diligence obligation on Member States to take appropriate measures to protect persons within their jurisdiction against reasonably foreseeable terrorism and bring the perpetrators of such acts to justice.[16]

Taking effective measures to protect the population against security threats while at the same time ensuring the protection of human rights in the context of preventing and countering terrorism and violent extremism may raise practical challenges for States. However, States can effectively meet their obligations under international law by using the flexibilities built into the international human rights law framework, in particular through the appropriate use of derogations and limitations.

In case of a state of emergency "threatening the life of the nation", States may lawfully derogate from certain human rights obligations, subject to a set of conditions.[17] Moreover, even outside of a state of emergency, States can impose limitations on the exercise of certain rights. Such limitations must be provided by law and necessary to protect a legitimate aim (such as national security, public order, public safety, or the rights and freedoms of others). Any measures must also be governed by the principles of necessity and proportionality and must respect the need for consistency with other guaranteed human rights.

These conditions defined under international human rights law to lawfully limit certain rights apply for example to the use of special investigative techniques by States. The Council of Europe has defined special investigative techniques as "techniques applied by the competent authorities in the context of criminal investigations for the purpose of detecting

14 Secretary-General's remarks at second high-level Conference of Heads of Counter-Terrorism Agencies of Member States. 28 June 2021. https://www.un.org/sg/en/content/sg/statement/2021-06-28/secretary-generals-remarks-the-second-high-level-conference-of-heads-of-counter-terrorism-agencies-of-member-states-delivered

15 United Nations Global Counter-Terrorism Strategy, A/RES/75/29 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/175/70/PDF/N2117570.pdf?OpenElement

16 Office of the United Nations High Commissioner for Human Rights, Human rights, terrorism and counter-terrorism, (OHCHR, Fact Sheet No. 32, 2008), Introduction, and paras. 19-20.

17 For example, Article 4 of the ICCPR provides for the possibility for States to temporarily adjust certain obligations under the treaty in time of "public emergency which threatens the life of the nation," provided a number of conditions are met, including that such measures be limited to the extent strictly required by the exigencies of the situation. This obligation reflects the principle of proportionality which is common to derogation and limitation powers. Any measures thus taken need to be in genuine response to the situation, aimed at the restoration of a constitutional order respectful of human rights and be fully justified by the circumstances. See also, Human Rights Committee, General Comment no. 29, States of emergency (Article 4), CCPR/C/21/Rev.1/Add.11. Other human rights covenants containing derogation clauses include the European Convention on Human Rights and the American Convention on Human Rights. However, many human rights treaties do not provide for the possibility to derogate from their provisions in case of states of emergency. These include, among others, the International Covenant on Economic, Social and Cultural Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention on the Elimination of All Forms of Discrimination Against Women and the African Charter on Human and Peoples' Rights.

and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target persons".[18] These include: 1) secret investigations with public interaction and without deception, such as informant or source recruitment; 2) secret investigations without public interaction and without deception, such as electronic surveillance; 3) secret investigations with public interaction and with deception, such as the use of undercover officers; and 4) secret investigations without public interaction but with deception, such as sting operations.[19]

However, in moving to meet their obligations to counter-terrorism, many States have rushed through legislation, adopted and implemented practices, that did not comply with their obligations under international human rights law and resulted in unlawful interference with human rights.[20]

In some cases, the consequences of problematic policies, legislation, and practices have been unintended, while in others, States have deliberately misused counter-terrorism measures to target political opposition, the media, civil society or human rights defenders or racial, ethnic, religious or other minorities. The impact of broadly defined or improperly applied counter-terrorism measures on civic space, the rule of law, or democratic processes is not a minor or academic concern. Although estimates vary, groups monitoring democratic space and civil society conditions across the globe agree that well over half of the world's population live in States where fundamental freedoms are either non-existent or substantially repressed.[21] Some of these States have adopted counter-terrorism measures granting authorities broad or unfettered surveillance powers, including the ability to monitor government critics, human rights defenders, anti-corruption activists, and journalists, or large segments of the population; the ability to restrict or shut down financial pipelines for civil society groups; the ability to limit access to individual or a substantial number of social media sites; the ability to force social media sites to remove legitimate content; the ability to shut down Internet access in an arbitrary manner; and the ability to control media houses and censor or discourage legitimate forms of expression. Online attacks have been shown to pave the way for human rights violations and abuses, including killings, torture, enforced disappearances, and arbitrary deprivation of liberty.[22]

Unlawful or arbitrary surveillance, unwarranted restrictions on legitimate expression, including through unlawful or arbitrary removal of online content, blocking of websites, cutting off Internet access, blocking circumvention technologies, and vague or overbroad laws criminalizing expression can have a deep chilling effect not only on freedom of expression, including the right to access to information, but also on interconnected public interest processes as well as the freedoms of peaceful assembly and association.

---

18 Council of Europe, Recommendation Rec(2005)10 of the Committee of Ministers to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, Definitions and Scope. https://www.refworld.org/pdfid/43f5c6094.pdf

19 Tom Parker, Avoiding the Terrorist Trap: Why Respect for Human Rights is the Key to Defeating Terrorism. Special Investigative Techniques, World Scientific Publishing Company, July 2, 2019.

20 Office of the United Nations High Commissioner for Human Rights, Human rights, terrorism and counter-terrorism, (OHCHR, Fact Sheet No. 32, 2008), Introduction, and para. 20. https://www.ohchr.org/en/publications/fact-sheets/fact-sheet-no-32-terrorism-and-counter-terrorism

21 Freedom House estimates that 20% of the global population live in countries that are free; 38% live in countries that are not free; and the remainder live in countries that are partly free. See, Freedom in the World, 2022. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf It also estimates that of the 4.5 billion people with access to the Internet, 76% live in countries where individuals were arrested or imprisoned for posting content on political, social, or religious issues. See, Freedom on the Net, Annual Survey 2022, available at https://freedomhouse.org/report/freedom-net/

Civicus estimates that 3.1% of the world's population live in countries with open civic space while 70% live in countries where civil society is either non-existent or repressed. <https://monitor.civicus.org/quickfacts/#:~:text=CIVIC%20SPACE%20IN%202022,decimal%20point%20to%20the%20percentages>

22 See: e.g., A/HRC/52/39; Position Paper of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach. See also US/EU Joint Statement on Protecting Human Rights Defenders. < https://www.eeas.europa.eu/eeas/useu-joint-statement-protecting-human-rights-defenders-online_en>

This guide references the human rights impact of a series of new technologies, including social media, the Dark Web, cryptocurrencies, and facial recognition technologies but does not address the full scope of use of artificial intelligence (AI) in countering terrorism or the use of remotely controlled weapons.

The use of new technologies in a counter-terrorism context has the potential to affect a broad range of human rights, including, but not limited to the right to privacy, the rights to freedom of expression and association, the right to political participation, the right to equal protection of the law without discrimination and fair trial rights. United Nations entities and mechanisms have in particular stressed the role of the right to privacy and freedom of expression in this regard as gateway rights that enable the exercise of a series of interconnected human rights.

Adopting and implementing laws, policies, and practices that are compliant with international human rights law is not only a legal obligation but also a strategic imperative for successful and sustainable counter-terrorism efforts. The General Assembly and the Security Council have long recognized that violations of human rights factor among the conditions conducive to terrorism and that States' failure to comply with their obligations under international human rights law is one of the factors contributing to increased radicalization to violence. Laws, policies, and practices contrary to such obligations are therefore counter-productive as they may fuel grievances that may be exploited by terrorists for recruitment purposes.

[IV] Overarching Considerations

4.1 Overview

Measures to prevent and counter-terrorism are frequently codified in a broad range of domestic regulatory instruments encompassing not only counter-terrorism legislation but also interconnected laws, rules, regulations, directives and proclamations such as codes on criminal law and procedure; laws on the Internet and telecommunications; cybersecurity laws; security legislation, including laws regulating the functioning of intelligence agencies; data protection laws; financial laws and regulations; etc. As counter-terrorism responses frequently result in the restriction of human rights, Member States have faced challenges in taking effective measures to address terrorism-related threats while fully complying with relevant obligations under international human rights law. However, the inbuilt flexibilities of the international human rights law framework[23] enable States to comply with their obligations to respect human rights while taking necessary and proportionate measures to address terrorist threats, including to ensure that any person who participates in the financing, planning, preparation, or perpetration of terrorist acts or in supporting such acts is brought to justice.

Specifically, under international human rights law it is possible for States to derogate from and to impose limitations on the exercise of certain rights. The conditions for derogations and limitations will be briefly set out below.

At the same time, some human rights are absolute. Such rights include the prohibitions on torture and cruel, inhuman, or degrading treatment or punishment, on slavery and servitude as well as the principle of legality requiring that there be no punishment without law. The absolute nature of these rights means that it is not permitted to restrict them by balancing their enjoyment against the pursuit of a legitimate aim, including in case of armed conflict, or any case of public emergency.

23 See, for example, OHCHR, Fact Sheet No. 32: Terrorism and Counter-Terrorism; K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 18.

4.2 Derogations

When facing a public emergency "threatening the life of the nation",[24] States have the possibility to temporarily adjust certain human rights obligations,[25] subject to a set of condition. As such, measures derogating from human rights must be limited to the extent strictly required by the exigencies of the situation and in genuine response to the threat in question, aimed at the restoration of a constitutional order and fully justified by the circumstances.[26] Moreover, adequate safeguards must be set up to protect against arbitrary and disproportionate interference with human rights[27] and procedural safeguards are not to be limited in a manner that would circumvent the protection of rights that cannot be subject to derogations.[28]

Derogation measures must not be inconsistent with a State's "other obligations under international law", particularly under international humanitarian law.[29] In this regard, a number of acts are prohibited at all times and therefore cannot be made subject to lawful derogations in a state of emergency. These include the prohibitions against the taking of hostages; unacknowledged detention; deportation or forcible transfer of a population without grounds permitted under international law, in the form of forced displacement by expulsion or other coercive means from the area in which the persons concerned are lawfully present; propaganda for war, or advocacy of national, racial, or religious hatred that would constitute incitement to discrimination, hostility, or violence.[30]

4.3 Limitations

Even outside of a state of emergency, States can impose limitations on the exercise of certain rights.[31] Such limitations must be provided by law and necessary to protect a legitimate aim (including national security, public order, public safety, or the rights and freedoms of others). Any measures must also be governed by the principles of necessity and proportionality, and respect the need for consistency with other guaranteed human rights.

24 The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism addressed Member States' practices related to exercising emergency powers in a counter-terrorism context and relevant human rights concerns. See, in this respect, A/HRC/37/52.

25 Note that the possibility to derogate during a state of emergency is only provided under certain human rights treaties. These include the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the American Convention on Human Rights. Other instruments do not provide for the option to adjust obligations due to the existence of a state of emergency, including the International Covenant on Economic, Social and Cultural Rights, or the African Charter of Human and Peoples' Rights.

26 Human Rights Committee, General Comment No. 29 'States of emergency (Article 4)', CCPR/C/21/Rev.1/Add.11. Please note that the mere fact that derogating from a specific treaty provision may, of itself, be justified by the exigencies of the situation does not obviate the requirement to demonstrate the necessity of the concrete measures taken pursuant to the derogation.

27 Human Rights Committee, General Comment No. 29 'States of emergency (Article 4)', CCPR/C/21/Rev.1/Add.11, para. 4.

28 This was set out by the Human Rights Committee both in General Comment no. 29 on States of emergency (Article 4)', CCPR/C/21/Rev.1/Add.11 and in its new General Comment no 35 on the liberty and security of person (Article 9), CCPR/C/GC/35 where the Committee unequivocally stated that habeas corpus was non-derogable (paras. 65-67).

29 Human Rights Committee, General Comment No. 29 'States of emergency (Article 4)', CCPR/C/21/Rev.1/Add.11, para. 9.

30 General Comment 29, para. 13.

31 Some human rights cannot be restricted. These include, in addition to the prohibitions of torture and cruel, inhuman or degrading treatment or punishment, of slavery and servitude, as well as the principle of legality (rights that are absolute). The absolute character of these rights means that it is not permitted to restrict them by balancing their enjoyment against freedom of thought, conscience and religion, as well as freedom of opinion. It has to be noted in this respect however that the right to manifest one's religion or beliefs as well as the right to freedom of expression may be limited in accordance with the conditions set by human rights law.

4.3.1 Legitimate Aim

Limitations of human rights must be necessary to protect legitimate aims, such as national security, public order/ public security, public health or morals, or the rights and freedoms of others. As such, specific rights should only be limited for the purposes set out in relation to the rights in question[32] and must be "directly related to the specific need on which they are predicated".[33] The Human Rights Committee noted that "interests of national security" may serve as a ground for restrictions "if such restrictions are necessary to preserve the State's capacity to protect the existence of the nation, its territorial integrity or political independence against a credible threat or use of force".[34] At the same time, in cases when the very reason that national security has deteriorated is the suppression of human rights, this cannot be used to justify further restrictions.[35] However, States have at times improperly referred to the imperatives of national security, specifically counter-terrorism, as a pretext to justify vaguely and define arbitrary interferences with human rights. This concern has been echoed by various United Nations human rights entities and mechanisms. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted the following:

"The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable grounds such as human rights defenders, journalists, or peaceful activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.[36]

4.3.2 Provided by Law

Any counter-terrorism measures that restrict human rights must have a basis in domestic law. That domestic legal basis much be sufficiently foreseeable, accessible, and provide adequate safeguards against abuse.

Foreseeability implies that the law must be formulated with sufficient precision to enable an individual to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail and regulate their conduct accordingly.[37] This requirement does not call for absolute foreseeability but rather that the law give individuals an "adequate indication as to the circumstances in which the conditions on public authorities are empowered to interfere with their rights".[38] The law must further provide sufficient guidance to those charged with its execution to enable them to ascertain when rights can be restricted and indicate the scope of any discretion conferred on the competent authorities as well as the manner of its exercise.[39] It must establish adequate safeguards against possible abuses such as an independent review and oversight. In case of violations of human rights, it must provide for an effective remedy. Finally, the requirement

32 The legitimate aims that justify restrictions are specific to the rights in question as set out in international and regional human rights treaties. For example, the freedom to manifest one's religion or beliefs may be subject to limitations prescribed by law and necessary to protect public safety, order, health, or morals or the fundamental rights and freedoms of others. Note that unlike for example freedom of expression or the right of peaceful assembly, the freedom to manifest one's religion or beliefs cannot be restricted in the interest of national security.

33 See, e.g., Human Rights Committee, General Comment No. 22, Article 18, CCPR/C/21/Rev.1/Add.4, para. 8; Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 22.

34 Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (E/CN.4/1985/4, annex), para. 29; Human Rights Committee, General Comment No. 37, Article 21 on the right of peaceful assembly, CCPR/C/GC/37, para. 42.

35 Ibid.

36 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, para. 58. < http://www.ohchr.org/Documents/HRBodies /HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf>

37 See, e.g., Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 25ff; European Court of Human Rights, *Sunday Times v. The United Kingdom (no. 1)*, Application no. 6538/74, 26 April 1979, § 49.

38 See, e.g., European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, §§ 66-68.

39 See, e.g., Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 25; European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, §§ 66-68.

that the law be sufficiently accessible entails that individuals that are to be affected by the respective legislation must have the possibility to become aware of its content (in most cases this requires accessibility to the public).[40]

With respect to government surveillance which may interfere with the right to privacy, for example, the European Court of Human Rights has considered that the requirement of foreseeability "cannot be exactly the same in the special context of interception of communications for the purposes of police investigations", further explaining that this requirement in this particular context "cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly". Nevertheless, the Court has held that: "[T] he law must be sufficiently clear in its terms to give citizens adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence". Consequently, "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measures in question, to give the individual adequate protection against arbitrary interference".[41] Secret rules, guidelines, or interpretations of the rules do not have the quality of "law".[42] A decision to make use of such authorized interference, for example, by issuance of a warrant, must be made only by an independent authority designated under the law, and on a case-by-case basis.[43]

4.3.3 Proportionality

Any interference with a qualified right must not only be taken in pursuance of a legitimate aim, it must also be necessary to protect the aim. The requirement of necessity sets a higher threshold than what is "merely reasonable or expedient". In essence, a measure violates the test of necessity if the protection could be achieved in other ways that do not restrict the right in question.

40 See, e.g., Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 25; European Court of Human Rights, *Groppera Radio AG and Others v. Switzerland*, Application no. 10890/84, Series A no. 173, 28 March 1990, §§ 65-68.

41 See, e.g., European Court of Human Rights, *Malone v. The United Kingdom*, Application no. 8691/79, 2 August 1984, §§ 67-68.

42 Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, para.29.

43 Human Rights Committee, General Comment No. 16, Article 17 (Right to privacy), para. 8.

Measures restricting a qualified right must be proportionate to the legitimate aim pursued; they must be appropriate to achieve their protective function and they must be the least intrusive means among those that might achieve the desired result, and they must be proportionate to the interest to be protected.[44] In this respect, addressing limitations to the right to privacy, the European Court of Human Rights held that "the blanket and indiscriminate" retention of DNA amounted to a "disproportionate interference" with the private lives of those persons from which the data had been taken. The Chamber placed particular weight on the fact that the material was "retained indefinitely" whatever the nature or seriousness of the offense of which the person was suspected, an especially appropriate consideration in the case as one defendant was acquitted and the case against the second was discontinued.[45]

4.3.4 Non-Discrimination

The prohibition against discrimination in international human rights law is absolute and there can be no derogation from or restriction on that right, whether in a state of emergency of outside of it.[46] Protected grounds comprise sex, race, colour, language, religion, political or other opinion, national or social origin, ethnic origin,[47] property, birth or other status.

As such restrictions on human rights must always respect the prohibition against discrimination.[48] Domestic law setting out the conditions under which human rights can be restricted therefore must contain adequate safeguards against discriminatory implementation.

4.3.5 Model Provisions on Consistency of Counter-Terrorism Practices with Human Rights and Refugee Law, and Humanitarian Law

The United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Special Rapporteur on Counter-Terrorism and Human Rights) has formulated a template concerning the consistency of State counter-terrorism conduct with international human rights law and refugee law as well as applicable provisions of international humanitarian law, as set out in the text box below.[49]

---

44 The Inter-American Court of Human Rights uses the term "adequate" rather than "proportionate." African Commission on Human and Peoples' Rights, Principles and Guidelines on Human and Peoples' Rights While Countering Terrorism in Africa, General Principle M. https://www.achpr.org/legalinstruments/detail?id=9

45 European Court of Human Rights, *S and Marper v. United Kingdom* (2009) 48 EHRR 50 at para 118. In this case, one of the accused was acquitted and the case against the second was discontinued. The UK government itself admitted that the retention of DNA data "was neither warranted by any degree of suspicion of the applicants' involvement in a crime or propensity to crime nor directed at retaining records in respect of investigated alleged offences in the past. Also on the principle of proportionality, see: Inter-American Court on Human Rights, *Roche Azaña v. Nicaragua* Merits and Reparations. Judgment of June 3, 2020. Series C No. 403, para. 53.

46 See, for example, Universal Declaration of Human Rights (arts. 1 and 2) and International Covenant on Civil and Political Rights (art. 26), as well as the Convention on the Elimination of Racial Discrimination (CERD). The Inter-American Court of Human Rights, for example, has stated that "the principle of equality before the law, equal protection before the law and non-discrimination belong to jus cogens, because the whole legal structure of national and international public order rests on it and it is a principle that permeates all law." Inter-American Court of Human Rights, Advisory Opinion OC-18/03 on the juridical condition and rights of the undocumented migrants, 17 September 2003, para. 101. African Commission on Human and Peoples' Rights, Principles and Guidelines on Human and Peoples' Rights While Countering Terrorism in Africa, General Principle G. the Committee on the Elimination of Racial Discrimination has called on States to ensure that any measures taken in the fight against terrorism do not discriminate, in purpose or effect, on the grounds of race, colour, descent, or national or ethnic origin and that non-citizens are not subjected to racial or ethnic profiling or stereotyping.

47 Although not included as protected ground in the International Covenant on Civil and Political Rights (art.26), "ethnic origin" is identified as an additional protected ground in Article 1 of the International Convention on the Elimination of All Forms of Racial Discrimination.

48 See, e.g., Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights (E/CN.4/1985/4, annex); Human Rights Committee, General Comment No. 37, Article 21 on the right of peaceful assembly, CCPR/C/GC/37, paras. 36, 46; Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 32.

49 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/16/51), Practice 2. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement

BOX 1. UN Special Rapporteur on Counter-Terrorism and Human Rights: Restrictions on Rights and Freedoms

1. The exercise of functions and powers shall be based on clear provisions of law that exhaustively enumerate the powers in question.
2. The exercise of such functions and powers may never violate peremptory or non-derogable norms of international law, nor impair the essence of any human right.
3. Where the exercise of functions and powers involves a restriction upon a human right that is capable of limitation, any such restriction should be to the least intrusive means possible and shall:
   - Be necessary in a democratic society to pursue a defined legitimate aim, as permitted by international law; and
   - Be proportionate to the benefit obtained in achieving the legitimate aim in question.
4. If the State is involved, as a party, in an ongoing armed conflict, the above provisions shall apply also to securing compliance with principles and provisions of international humanitarian law, without prejudice to the obligation to comply with international human rights and refugee law.
5. If compelling reasons require the establishment of specific powers for certain authorities:
   - Such powers should be contained in stand-alone legislation capable of being recognized as a unique exception to customary legal constraint;
   - The provisions under which such powers are established should be subject to sunset clauses and regular review; and
   - The use of such powers for any purpose other than the combating of terrorism must be prohibited.

[V]

Definitions of Terrorism and Incitement to Terrorism

5.1 Definition of Terrorism

United Nations human rights mechanisms and other stakeholders have repeatedly raised concerns about the implications of overly broad definitions of terrorism and related offences[50] that have at times encompassed manifestations that are protected under international human rights law.

The prerequisites for a human rights compliant counter-terrorism effort includes a legal and policy framework grounded in clear and precise definitions of terrorism and related offences, including incitement to terrorism. These definitions must not be so broad or vague as to cover non-violent acts or legitimate speech including dissent, criticism, or non-conformism. Imprecise laws have often been exploited to label civil society actors as terrorists and to prosecute them for terrorism-related offences. Other counter-terrorism measures and laws have been introduced to restrict civil society access to funding, thereby resulting in curbs on their activities.[51]

Paragraph 3 of Security Council Resolution 1566 (2004) sets out terrorism as encompassing "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism".[52]

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (Special Rapporteur on counter-terrorism and human rights) has proposed a similar model definition, reflecting best practice in countering terrorism, pursuant to an analysis undertaken on the basis of consultations and various forms of interaction with multiple stakeholders, including Governments.[53]

50 See, for example, Protecting human rights and fundamental freedoms while countering terrorism. Report of the Secretary-General. (A/68/298); Report of the United Nations High Commissioner for Human Rights on the protection of human rights and fundamental freedoms while countering terrorism. (A/HRC/28/28); International Commission of Jurists. (2009). Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights.

51 Report of the Secretary-General on Terrorism and Human Rights, A/76/273 (2021), paras. 22, 24. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/218/29/PDF/N2121829.pdf?OpenElement

52 Also relevant is the definition of terrorism set out in General Assembly Resolution 51/210: "...criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes... whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them."

53 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 2010, A/HRC/16/51. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/178/98/PDF/G1017898.pdf?OpenElement

BOX 2. Terrorism Definition

Terrorism means an action or attempted action where: 1. The action: (a) Constituted the intentional taking of hostages; or (b) Is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or (c) Involved lethal or serious physical violence against one or more members of the general population or segments of it; the action is done or attempted with the intention of: (a) Provoking a state of terror in the general public or a segment of it; or (b) Compelling a Government or international organization to do or abstain from doing something; and (3) The action corresponds to: (a) The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or (b) All elements of a serious crime defined by national law.

Both paragraph 3 of Security Council 1566 (2004) and the model definition developed by the mandate of the Special Rapporteur on counter-terrorism and human rights limit the scope to conduct that is aimed at a) terrorizing or otherwise seriously intimidating the general population or a segment of it, and b) unlawfully coercing a government or an international organization to do or abstain from doing something.

The mandate of the Special Rapporteur on counter-terrorism and human rights has consistently emphasized the importance of restricting counter-terrorism definitions and measures derived therefrom to conduct that is truly terrorist in nature. In this vein, all counter-terrorism laws "must be limited to the countering of offences within the scope of, and as defined in, the international conventions and protocols relating to terrorism, or the countering of associated conduct called for within resolutions of the Security Council, when combined with the intention and purpose elements identified in Security Council Resolution 1566 (2004)."[54] In particular, "[c]rimes not having the quality of terrorism (...), regardless of how serious, should not be the subject of counter-terrorist legislation."[55]

BOX 3. The Mandate of the Special Rapporteur has Further Developed a Model Definition Based on Best Practice for the Offence of Terrorist Incitement

It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.[56]

The protection of freedom of expression under international human rights law extends to speech that may be deeply offensive to some.[57] At the same time certain forms of expression that cannot genuinely be characterized as terrorist and would not fall within the scope of the above definition, may nonetheless be unlawful. In particular, such content may amount to advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence and should be addressed in line with Articles 20 and 19(3) of the International Covenant on Civil and Political Rights and the standards spelled out in the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.[58]

54 E/CN.4/2006/98, para. 39.

55 *Ibid*. para. 47.

56 A/HRC/16/51, Practice 8.

57 Human Rights Committee, General Comment No. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, para. 11.

58 A/HRC/22/17/Add.4, in particular its para. 29.

BOX 4. The IACHttR* Decision on the Definition of Terrorism

The counter-terrorism legislation of **Country X** included a provision establishing that "unless the contrary is verified, the intent of causing fear to the general population shall be presumed when the offense is committed using explosive or incendiary devices…"

The Inter-American Court of Human Rights held that this formulation which included a presumption of intent violated the cornerstone principle of the presumption of innocence as well as the principle of legality.

Norín Catrimán et al v. Chile, paras. 170–171, and 174.
* The Inter-American Court of Human Rights

BOX 5. The ECtHR* on the Quality of Domestic Law

In a case against Turkey, the Court observed that it was "mindful of the difficulties linked to preventing terrorism and formulating anti-terrorism criminal laws…Member States inevitably have recourse to somewhat general wording" that is to be interpreted by the courts who "must give the individual adequate protection against arbitrary interference". The Court noted that the Council of Europe Commissioner for Human Rights observed that it was increasingly common in Turkey for the evidence used to justify detention to be solely limited to statements and acts that were "manifestly non-violent" noting that domestic courts often relied on extremely weak evidence when authorizing pre-trial detention on charges of membership in an armed organization. The Court concluded that the range of acts that may have justified the applicant's pre-trial detention in connection with serious offences criminalized under Turkey's Criminal Code as membership in an armed organization, coupled with judicial interpretations, did not afford adequate protection against arbitrary interference with protected rights. The Court noted that the broad interpretation of "a provision of criminal law cannot be justified where it entails equating the exercise of the right to freedom of expression with belonging to, forming or leading an armed terrorist organization, in the absence of any concrete evidence of such a link." On this basis it held that the interferences with the applicant's freedom of expression did not comply with the requirement of the quality of the law.

Selahattín Demírtas v. Turkey (No.2), paras. 279-281.
* The European Court of Human Rights

5.1.1 Definition of Incitement to Terrorism

United Nations Security Council Resolution 1624 calls on States to enact laws prohibiting incitement to terrorism but does not include a definition of incitement. The Special Rapporteur on counter-terrorism and human rights has suggested the following model definition:

> It is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.

BOX 6. ECtHR* Finds That Conviction for Condoning Terrorism Does Not Violate the Applicant's Freedom of Expression

The applicant, a cartoonist, was convicted of condoning terrorism following the publication of a drawing representing the attack on the World Trade Center with a caption stating: "We all dreamt of it...Hamas did it."

The Court considered that the drawing was not limited to criticism of American imperialism but commented approvingly of violence perpetrated against thousands of civilians. The Court also observed approvingly that only a modest fine had been imposed on the perpetrator.

Leroy v. France, paras. 43, 47.
*The European Court of Human Rights

[VI]
Online Surveillance and Privacy

6.1 International Human Rights Law Norms and Standards Relevant to Surveillance Measures

The right to privacy is protected under international and regional human rights treaties. Article 17 of the International Covenant on Civil and Political Rights provides for the following:

> **"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".**

The right to privacy is also protected under Article 8 of the European Convention for Human Rights, and Article 11 of the American Convention on Human Rights. The African Commission on Human and Peoples' Rights has asserted that components of the right to privacy can be inferred from the African Convention on Human and Peoples' Rights.[59] The seventh review resolution of the United Nations Global Counter-Terrorism Strategy urged Member States to "respect the right to privacy, [...] including in the context of digital communication while countering terrorism, and to take measures to ensure that interferences with or restrictions on that right are not arbitrary or unlawful and are subject to effective oversight and to appropriate redress, including through judicial review or other legal means".[60]

Interference with privacy rights to aid law enforcement and intelligence agencies in the protection of public order, public safety or national security can be consistent with international human rights law in case relevant measures are provided by law, necessary and proportionate. New technologies have dramatically expanded the forms of surveillance available as information is no longer confined to locked rooms but may be held on computers, phones, social media accounts, geolocation devices, etc. The Constitutional Court of South Africa observed that: "[t]oday technology enables law enforcement agencies to not only physically – as opposed to electronically – invade the 'intimate personal sphere' of people's lives, but also to maintain and cement its presence there, continuously gathering, retaining and – where deemed necessary – using information".[61]

59 African Commission on Human and Peoples' Rights, Principles and Guidelines on Human and Peoples' Rights While Countering Terrorism in Africa, Section 11. https://www.achpr.org/legalinstruments/detail?id=9

60 A/RES/77/298, para. 11.

61 Constitutional Court of South Africa, *In the matter of Amabhungane Centre for Investigative Journalism*, Case CCT 278/19, para. 2. < https://privacyinternational.org/sites/default/files/2021-02/%5BJudgment%5D%20CCT%20278%20of%2019%20and%20279%20of%2019%20AmaBhungane%20Centre%20for%20Investigative%20Journalism%20v%20Minister%20of%20Justice%20and%20Others.pdf>

BOX 7. THE ECtHR* on Secret Surveillance

In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on (...) the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."

Big Brother Watch and Others v. the United Kingdom
* The European Court of Human Rights

BOX 8. Example of Data Collection Legislation Granting Excessive Powers to Surveil to Law Enforcement

In Member State F, new cybersecurity legislation requires all online platforms to retain data of its citizens usernames, birth dates, nationality, identity cards, credit card numbers, biometric files, and health records. Authorities can access the data on vaguely defined national security and public order grounds.

As early as 1978, the European Court of Human Rights considered the dangers of unregulated surveillance in combatting terrorism observing that "[t]he Court, being aware of the danger [that unregulated surveillance] poses of undermining or even destroying democracy on the ground of defending it, affirms that [...] States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[62] It also noted that the risks of arbitrariness and abuse are inherent in any system of secret surveillance and that since the implementation of secret surveillance measures is not open to scrutiny by the individuals concerned or the public at large, unfettered discretion cannot be granted to the executive or a judge.[63]

Similarly, the Inter-American Court expressed fear that "[l]aws that authorize the interception and monitoring of... communications that were formulated to combat crime, can become an instrument for spying and harassment if they are interpreted and applied improperly. Hence, owing to the inherent danger of abuse in any monitoring system, this measure must be based on especially precise legislation with clear, detailed rules" It further stated that "the surveillance, intervention, recording and dissemination of communications is prohibited, except in the cases established by law that are adapted to the objects and purposes of the American Convention.[64]

These fears have been borne out, as around the globe national authorities in several Member States have been shown to employ both old and new technologies to unlawfully or arbitrarily monitor the activities of journalists, human rights defenders, anti-corruption whistleblowers, student activists, dissidents, and other categories of individuals considered a nuisance or threat to government policies or the legitimacy of particular governments.

New technologies and data collection methods have a disparate impact on minorities and are profoundly gendered. The family and home space are often part and parcel of those surveillance measures and the unlawful use of counter-terrorism measures has also demonstrated patterns of targeting whole families, with a direct impact on the right to privacy. Women, for example, may immediately be presumed to be suspect by virtue of familial or communal association with particular men. Mothers and wives are invariably conflated with the violent acts of their children or husbands, with their homes being often the target of intrusive and violent State searches; and them frequently becoming the objects of

62 European Court for Human Rights, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, para. 49.

63 See for example, European Court of Human Rights, *Roman Zakharov v. Russia*, paras. 299-231.

64 Inter-American Court on Human Rights, *Escher v. Brazil*, para. 118.

ongoing surveillance and harassment. Surveillance laws have also been widely misused and abused to target particular communities and groups based on ethnic background, race and religion.[65]

With respect to the surveillance of digital communications, the General Assembly called on states to enact legal frameworks which are publicly accessible, clear, precise, comprehensive and non-discriminatory.[66] The Human Rights Council elaborated on these issues in its Resolution 42/15 on the right to privacy in the digital age, calling on States to:[67]

- Ensure that measures taken to counter-terrorism and violent extremism conducive to terrorism that interfere with the right to privacy are consistent with the principles of legality, necessity and proportionality;
- Establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, and accountability for State surveillance of communications, their interception and the collection of personal data; and
- Develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful or arbitrary collection, processing, retention or use of personal data by individuals, Governments, business enterprises and private organizations.

The guidance set by the European Court of Human Rights contains further useful details in this respect. The court has identified the following minimum safeguards a surveillance law must meet in order to be compatible with the right to respect for private and family life:[68]

- The nature of offences which may give rise to an interception order must be spelled out in a clear and precise manner;
- The law must clearly indicate which categories of people may be subject to surveillance;
- There must be strict time limits on surveillance operations;
- Procedures must be in place for ordering the examination, use, storage, and retention of the data obtained through surveillance
- The law must lay down the precautions to be taken when communicating data to third parties;
- There must be regulation on the retention of intercepted information; the fact that a piece of information may one day be useful, does not justify the retention of thousands of pieces of such information indefinitely; and
- There must be independent bodies responsible for oversight of surveillance programmes.

65 See, e.g., A/HRC/46/36. para. 11 and 26.

66 A/Res/ 73/179.

67 A/HRC/RES/42/15, para. 6.

68 Article 8 of the European Convention on Human Rights. See also, Brief of Amici Curiae Article 19, Electronic Frontier Foundation, Fundación Karisma, and Privacy International at the Inter-American Court for Human Rights in *Members of José Alvear Restrepo Lawyers' Collective v. Colombia*, p. 17; ECHR, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, paras. 42 and 49, *Liberty and Others v. the United Kingdom*, no. 58243/00,1 July 2008 and *Rotaru v. Romania*, no. 28341/95,[GC], 4 May 2000 concerning surveillance carried out by the intelligence agencies.

The Special Rapporteurs on Freedom of Expression of the United Nations and the Organization of American States (OAS) issued a joint declaration in which they took a similar approach:[69]

> States must guarantee that the interception, collection and use of personal information, including all limitations on the right of the affected person to access this information, be clearly authorized by law in order to protect them from arbitrary or abusive interference with their private interests. The law must establish limits with regard to the nature, scope and duration of these types of measures; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged.
>
> Given the importance of the exercise of these rights for a democratic system, the law must authorize access to communications and personal information only under the most exceptional circumstances defined by legislation. When national security is invoked as a reason for the surveillance of correspondence and personal information, the law must clearly specify the criteria to be used for determining the cases in which such surveillance is legitimate. It shall be authorized only in the event of a clear risk to protected interests and when the damage that may result would be greater than society's general interest in maintaining the right to privacy and the free circulation of ideas and information. The collection of this information shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight within the limitations permissible in a democratic society.

69 Joint Declaration on surveillance programs and their impact on freedom of expression, issued by the United Nations Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, June 2013, paras. 8 and 9. < http://www.oas.org/en/iachr/expression/showarticle.as p?artID=927&lID=1>.

BOX 9. **The ECtHR* Finds Absence of Sufficient Guarantees Against Abuse in Surveillance Legislation**

In assessing a State's surveillance legislation, the Court laid out the dangers of modern surveillance observing that "it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents....[however], it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives....The risk that a system of secret surveillance set up to protect national security [might even] undermine or even destroy democracy under the cloak of defending it...Where a power vested in the executive is secret, the risks of arbitrariness are evident". Consequently, the Court concluded that the scope and manner of the exercise of discretion had to be set out with clarity in controlling legislation.

In considering the State's compliance with this principle, the Court observed that in the State at issue almost any person in the State could be subject to surveillance as the legislation did not require authorities seeking authorization for surveillance to demonstrate an actual or presumed relationship between the target of the surveillance and the prevention of a terrorist threat. The absence of the requirement that an applicant for permission to surveil provide a factual basis for the application rendered irrelevant the approval process as there was no basis on which to evaluate the necessity of the intrusive measures which would ordinarily be based on suspicion regarding the individual target. The Court also noted that the law did not provide for judicial authorization of warrants or their renewal, and that instead authorization was provided by the Ministry of Justice rather than an independent body. The Court further expressed concern about the absence of provisions regarding the possibility of redress for those unlawfully subject to secret surveillance as well as the absence of independent oversight mechanism. The Court was also not satisfied that provisions for data storage, processing, and deletion were workable in the circumstances.

Thus, the Court concluded that the legislation did not provide sufficiently precise, effective, and comprehensive safeguards with respect to the ordering and execution of surveillance measures, as well as potential measures for redress.

Szabó and Vissy v. Hungary
*The European Court of Human Rights

6.2 Metadata / Bulk Surveillance

Metadata (communications data) is generally defined as "a set of data that describes and gives information about other data". It was initially believed that the collection of metadata relating to communications was of lesser concern than the collection of the content of communications. However, due to developments in technology, metadata, including the identification of the owner of an IP address, subscriber data, mobile device identifier or an email's IP address, a mobile subscriber identifier (IMSE), and email addresses can be highly revealing in an ecosystem where individuals leave their electronic footprints behind in their digital content. As such, metadata can be a proxy for content, and as a result, the collection and use of such data can be highly intrusive.[70] As a result, any distinctions between metadata and content may be increasingly difficult to justify as consistently highlighted by international and regional human rights

70 Brief of Amici Curiae Article 19, Electronic Frontier Foundation, Fundación Karisma, and Privacy International at the Inter-American Court for Human Rights in *Members of José Alvear Restrepo Lawyers' Collective v. Colombia*, p. 10. https://www.law.berkeley.edu/wp-content/uploads/2022/05/Amicus-Brief-CCAJAR-v.-Colombia.pdf

mechanisms and entities. The United Nations High Commissioner for Human Rights noted that metadata "may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication"[71] and noted that stronger protection of privacy requires equivalent protection of metadata. Similar developments have been reflected in the case law of the European Court of Human Rights and the Inter-American Court of Human Rights, among others.[72]

With respect to the bulk collection and use of metadata by security and intelligence agencies, the Court of Justice of the European Union has concluded that "data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[73]

In the case at issue, it observed that the impugned legislation requiring the indiscriminate retention of indiscriminate bulk data did not require any relationship between the data to be retained and a threat to public security.[74] Consequently, it held that national legislation requiring providers of electronic communications services to carry out the general and indiscriminate retention of such data for the purposes of safeguarding national security was unlawful.[75] With respect to national agencies seeking access to such data, the Court held that "general access to all retained data (by private companies), regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary" and therefore that access can only be granted to "data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime," and that such access further required prior judicial or independent administrative authorization.[76]

It added, however, that a State could adopt legislation permitting the targeted retention of traffic and location data, as a preventive measure and for the purpose of fighting serious crime, provided that "the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary".[77]

71 A/HRC/27/37, para. 19.

72 See, for example, Big Brother Watch and Others v. the United Kingdom [GC], *nos. 58170/13, 62322/14 and 24960/15*, Judgment, 25 May 2021; Escher et al. v. Brazil, Judgment, 6 July 2009.

73 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, para. 99.

74 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, paras. 103, 106.

75 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, para. 107

76 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, para. 119, 125.

77 Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others, para. 108.

6.3 Authorization, oversight and remedies

BOX 10. General Assembly Resolution 75/176* on the Right to Privacy in the Digital Age

The resolution calls on Member States, inter alia, to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data...

and provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations.

In its General Comment no. 16 on Article 17 (Right to Privacy), the Human Rights Committee noted that the authorization of an interference with the right to privacy, including surveillance measures, must be made only by the authority designated under the law and on a case-by-case basis.[78] The European Court of Human Rights has indicated that the body competent to authorize surveillance measures need not necessarily be a judicial body but such a non-judicial body must be sufficiently independent from the executive. The Court at the same time noted that an interference by the authorities with an individual's rights should be "subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure".[79]As highlighted by the Human Rights Committee, such authorizations must be made on a case-by-case basis.[80] Moreover, authorization must be grounded on facts. For example, in *Escher v. Brazil*, the Inter-American Court of Human Rights expressed concerns about a domestic court having authorized surveillance despite the fact that the request for surveillance did not include any reasons or grounds to justify it. It also observed that the those seeking permission had not indicated that less intrusive means of obtaining the information sought were unavailable.[81]

BOX 11. Tshwane Principle[82]* 10. E

The overall legal framework concerning surveillance of all kinds, as well as the procedures to be followed for authorizing surveillance, selecting targets of surveillance, and using, sharing, storing, and destroying intercepted material, should be accessible to the public.

78 General Comment 16, para. 8.

79 See, e.g., Szabó and Vissy v. Hungary, para. 77.

80 General Comment 16, para. 8.

81 Paras. 92, 134, 135, 140. The European Court of Human Rights has also held that "where a judge merely endorses the actions of security services without genuinely checking the facts or providing adequate oversight" there is a violation of Article 8 of the Convention. See *Zoltán Varga v. Slovakia*, paras. 155-160.

82 The Tshwane Principles on National Security and the Right to Information issued in June 2013 provide guidance to legislators and relevant officials engaged in the drafting, revising or implementing laws or provisions relating to states' authority to withhold information on national security grounds or to punish the disclosure of such information Based on international and national law, standards and practices, they were drafted, following extensive consultations facilitated by the Open Society Justice Foundation, with the involvement of a wide range of experts from governments, the national security sector, international organizations, civil society and academia. Four United Nations Special Procedures mandate holders, including the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism contributed to the consultations. The Parliamentary Assembly of the Council of Europe endorsed the Principles in October 2013, urging Council of Europe's member States to take them "into account in modernizing their legislation and practice" (resolution 1954 (2013)).

In line with international human rights norms and standards, surveillance should only be authorized for a finite period, although authorization may be renewed or extended if the continued necessity and proportionality of the measures can be demonstrated. Additionally, authorization must be explicit. Thus, for example, if authorization is only provided to collect data from a target's phone, data from the target's computer cannot be collected.

The European Court of Human Rights has addressed telephone tapping in a number of cases. The safeguards set out by the Court to ensure that such measures are conducted in line with human rights norms and standards are also applicable to other forms of surveillance, including online surveillance, are applicable to all forms of online surveillance. Authorizations for surveillance should include the following:

- The details of individuals whose communications are to be surveilled;
- The nature of the offences justifying the tapping;
- The duration of the surveillance;
- The procedure for drawing up the summary reports of intercepted communications;
- The precautions to be taken in order to maintain the integrity of intercepted communications; and
- The circumstances, including a time-limit, in which the information intercepted is to be erased or destroyed, for example, following the discharge or acquittal of the accused.[83]

6.3.1 Oversight Mechanisms[84]

The Human Rights Committee has noted that surveillance measures, including the interception of personal communications, and hacking techniques must be subject to clearly defined safeguards from abuse that must include robust and independent oversight systems.[85]

Oversight of security sector actors may take different forms, including internal oversight, independent external oversight (non-judicial and judicial), and parliamentary oversight.[86]

The first degree of control in any law enforcement accountability system is the internal control mechanisms within the police service. Effective controls assist in preventing misconduct and addressing it. Such mechanisms have three main components:

- Professional and integrity standards;
- Ongoing supervision and monitoring; and
- Internal reporting and disciplinary measures.

It is therefore imperative that police services develop comprehensive professional standards (codes of conduct, codes of ethics), providing clear guidance on the exercise of policing duties and powers in practice.

83 See See *Huvig v. France, 24 April 1990, § 34, Series A no. 176 B and Kruslin v. France, 24 April 1990, § 35, Series A no. 176-A;* ECtHR, *Greuter v. The Netherlands*, Application no. 40045/98, 19 March 2002.. Also, see OSCE/ODIHR, Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers, footnote 48 citing Countering Terrorism, Protecting Human Rights: A Manual, p. 205,/e

84 See United Nations Office on Drugs and Crime, https://www.unodc.org/e4j/en/crime-prevention-criminal-justice/module-5/key-issues/2—key-mechanisms-and-actors-in-police-accountability-and-oversight.html

85 CCPR/C/ITA/CO/6, para. 37. See also General Assembly Resolution 73/179.

86 Council of Europe, Police Oversight Mechanisms in the CoE Member States, Section 3, p. 67, available at: < https://rm.coe.int/police-oversight-mechanisms-in-the-coe-member-states/16807175dd>

The judiciary is an indispensable element of a police accountability system. Surveillance or covert data collection activities must be authorized or supervised by a judicial representative or body, or similarly independent mechanism, prior to the start of such activities, to the extent possible. The European Court of Human Rights has considered that in the field of surveillance where abuse is potentially so easy in individual cases and could have such harmful consequences for a democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.[87] The Court has expressed the view that either the body issuing authorisations for interception should be independent or there should be control by a judge or an independent body over the issuing body's activity. Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny.[88] In some civil law systems, investigative judges monitor law enforcement activities while they are ongoing. And in all systems, the judiciary is charged with adjudicating allegations of police misconduct and imposing sanctions and remedies.

One of the most fundamental roles of parliaments across the world is to draft, amend and enact laws. Thus, such bodies must establish comprehensive legal frameworks on law enforcement surveillance programmes that are in line with international law and human rights standards. Additionally, as legislative bodies are responsible for checking the powers of the executive branch, they often establish permanent or ad hoc oversight committees and inquiries to review covert or surveillance programmes.

Some Member States have also established independent expert bodies or data protection authorities specifically to oversee surveillance programmes. The precise form of the oversight body is not regulated by international law, but such bodies must be independent, be adequately resourced in terms of budgets, expertise, material, and must have robust powers set out in the law, including initiating and conducting independent investigations with full and unhindered access to information, installations and officials as well as the power to order the termination of collection measures.[89]

Independent oversight bodies should have access to the products of surveillance and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the relevant oversight bodies, and they should be required to keep records of all surveillance measures taken.[90] Oversight mechanisms may make recommendations for institutional and legislative reform that should be given appropriate consideration by the relevant executive and legislative bodies.

6.3.2 Right to an effective remedy

Article 2 of the International Covenant on Civil and Political Rights establishes that:

> (a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity; (b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative, or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; and (c) To ensure that the competent authorities shall enforce such remedies when granted.

87 European Court of Human Rights, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, para. 56.

88 European Court of Human Rights, *Dumitri Popescu v. Romania*, no. 71525/01, 26 avril 2017, para. 70-73; European Court of Human Rights, *Szabó and Vissy v. Hungary*, no. 37138/14, para. 77.

89 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, A/HRC/14/46, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

90 Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/39/29, para. 40, available at: < https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>

Such remedies may include, but are not limited to, fines and sanctions on the relevant individual or body engaged in unlawful conduct, as well as compensation to the victim(s). In order to make this right practicable, there is growing consensus that individuals should be entitled to post facto information regarding surveillance activities targeting them.

Effective remedies involve that any individual who believes that their rights have been infringed should also be able to bring a complaint to a court or oversight institution that can provide an effective remedy, including full reparation for the harm suffered. This may include non-judicial institutions empowered to receive and investigate complaints as well as to issue binding orders or provide effective remedies, or judicial institutions that can order remedial action. These institutions should be independent of the law enforcement agencies and the political executive, have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.[91] The European Court of Human Rights has clarified that in the context of secret surveillance an effective remedy means "a remedy that is effective as can be having regard to the restricted scope of recourse inherent in such a system".[92] In order to make this right practicable, there is growing consensus that individuals should be entitled to post facto information regarding surveillance activities targeting them. While noting that individuals are of necessity deprived of the possibility to challenge specific measures ordered or implemented against them while they are under way, the Court has further indicated that "this does not mean that it is altogether impossible to provide a limited remedy [...] even at this stage".[93]

6.4 Special Investigative Techniques

Special investigative techniques are typically characterized as operational resources that can be deployed both pre-emptively and reactively in the context of detecting and investigating serious crimes and suspects, with the aim of gathering information in such a way as not to alert the target persons.[94] The use of SITs may also involve a degree of deception. The Council of Europe has developed a typology of Special Investigation Techniques that identifies four distinct categories of such activity:[95]

1. Secret investigations with public interaction and without deception (e.g. informant operations);
2. Secret investigations with public interaction and with deception (e.g. undercover operations);
3. Secret investigations without public interaction but with deception (e.g. sting operations); and
4. Secret investigations without public interaction and without deception (e.g. eavesdropping).

91 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, A/HRC/14/46, para. 16-17, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement. See also: Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, para. 40-41.

92 European Court of Human Rights, *Klass and Others v. Germany*, no. 5029/71, 6 September 1978, para. 50 and 69

93 European Court of Human rights, *The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, 28 June 2007, para. 99-100.

94 Council of Europe, Recommendation Rec(2005)10 of the Committee of Ministers on "special investigation techniques" in relation to serious crimes including acts of terrorism (SIT Recommendation), 20 April 2005.

95 This typology was developed from the work of Professor G. Marx and Professor de Valkeneer. See Council of Europe, Terrorism: Special Investigation Techniques (April 2005), pp. 13-15.

As set out in the introduction, the use of Special Investigative Techniques (SITs) – including reliance on the on and offline recruitment of sources or the on and offline use of deceptive practices - can be both needed for the purposes of gathering intelligence and investigating serious crimes, including terrorism. However, the use of such techniques interferes with the privacy rights of those subjected to them and in some cases also that of third parties. The deployment of SITs may also impact other rights such as due process and fair trial rights. Consequently, Member States must define in their national legislation the circumstances in which, and the conditions under which, the competent authorities are empowered to resort to the use of special investigation techniques with due consideration for the human rights implications linked to their intrusive nature.

In addition:

- Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals.
- Competent authorities should apply the least intrusive investigation methods that enable the offence to be detected, prevented or prosecuted with adequate effectiveness and only resort to special investigative measures when less intrusive methods are not fit for purpose.
- Proportionality between the effects of the use of special investigation techniques and the objective that has been identified should be ensured. In this respect, when deciding on their use, an evaluation in light of the seriousness of the offence and taking account of the intrusive nature of the specific special investigation technique used should be made.
- Member States should, in principle, take appropriate legislative measures to permit the production of evidence gained from the use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.[96]

Finally, in relying on deceptive practices, law enforcement officers must distinguish between practices that will enhance evidence collection and those that may induce the commission of a crime. The latter, including the use of agents provocateurs or entrapment of suspects, may compromise the integrity of the evidence, thus leading to its inadmissibility in court. This also applies to undercover operations conducted online, for instance through the infiltration of specific forums believed to promote violent extremism.

Entrapment takes place when the police:

- Provide a person with an opportunity to commit a crime without having reasonable suspicion that the person is already engaged in criminal activity or with other good cause; and
- Although having such reasonable suspicion or other good cause, induce the commission of an offence.

In relation to such practices, the European Court of Human Rights Court stressed the crucial difference between officers concealing their identities in order to obtain information and evidence about a crime and actively inciting an individual to commit it and noted: "while the rise in organized crime undoubtedly requires that appropriate measures be taken, the right to a fair administration of justice nevertheless holds such a prominent place [...] that it cannot be sacrificed for the sake of expedience".[97]

96 Council of Europe Committee of Ministers, Recommendation Rec(2005)10 on "special investigation techniques" in relation to serious crimes including acts of terrorism.

97 Teixeira de Castro v. Portugal, European Court of Human Rights, Application no. 44/1997/828/1034, Judgment, 9 June 1998 § 36.

Thus, in order to ensure the admissibility of evidence and the right to a fair trial, deceptive practices must stop short of entrapment.[98]

BOX 12. Human Rights Compliant Use of SITs*

- Judicial authorities or other independent bodies should exert adequate control of the use of SITs, either through prior authorization, supervision during the operation, or ex-post facto review. The nature and level of control will depend on the degree of intrusiveness involved;
- SITs should be used only in serious cases;
- SITs should be used proportionally, based on the seriousness of the matter being investigated, and the degree of their intrusiveness should be a major consideration;
- Where the objective of the operation can be achieved "with adequate effectiveness" by use of less intrusive means or by non-SITs, this should always be the preferred option;
- The procedural rules governing the production and admissibility of evidence obtained by SITs should safeguard the right to a fair trial; and
- Those involved in the operational use of SITs should receive adequate training.

* Organization for Security and Cooperation in Europe, Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers, p. 32. <osce.org/odihr/108930>

98 Organization for Security and Cooperation in Europe, Human Rights in Counter-Terrorism Investigations: A Practical Manual for Law Enforcement Officers, pp. 40-45. <osce.org/odihr/108930>

[VII]

Facial Recognition, Privacy and Non-Discrimination

7.1 Facial Recognition

In Resolution 2396, the Security Council decided that Member States should "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law".

Whereas biometric tools have the potential to substantially contribute to making counter-terrorism efforts more targeted, more precise, and thereby more efficient,[99] "[t]hese technologies present complex legal and policy challenges that are relevant both to States' efforts to counter-terrorism and to their human rights obligations".[100] As also highlighted in the 2018 Addendum to the 2015 Madrid Guiding Principles acknowledging that the implementation of the requirements of resolution 2396 "requires legal frameworks, skills, capacity, expertise and equipment that [some Member States] do not currently possess".[101]

Indeed, the collection, retention, processing, transfer and other use of biometric data, as data relating to the physical, physiological or behavioural characteristics of a person, must be subject to adequate legislative and operational safeguards. In particular, such data should be collected and handled in line with applicable international human rights norms and standards as well as recognized data protection principles.[102]

AI powers the use of biometric technologies which are used for verification and identification purposes by public and private actors. Biometric recognition relies on the comparison of the digital representation of certain features of an individual, such as the face, fingerprint, iris, voice or gait, with other such representations in a database.[103] From the comparison, a higher or lower probability is deduced that the person is indeed the person to be identified.[104]

99 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 14.

100 S/2018/1177.

101 Ibid.

102 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 16.

103 European Parliamentary Research Service, Regulating Facial Recognition in the European Union. <https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf>

104 The Report of the High Commissioner of Human Rights, the Right to Privacy in the Digital Age, A/HRC/48/31. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement>

Facial Recognition refers to a multitude of technologies that can perform different tasks for different purposes. In considering the regulation of facial recognition responses, it is critical to distinguish between technologies designed to verify and those designed to identify.[105] Verification is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown in the two images is the same person. This type of verification is used, for example, at Automated Border Control gates at airports for border checks. A person scans his or her passport image and a live image is taken on the spot. The facial recognition technology compares the two facial images and if the likelihood that the two images show the same person is above a certain threshold, the identity is verified. This type of verification does not demand that the biometric features be deposited in a central database. They may be stored, for example, on a card or in an identity/travel document of an individual.[106]

Facial Recognition technologies designed to identify compare an individual's facial image with other images in order to try to identify the individual. Facial recognition technologies score each comparison and indicate a probability percentage that two images are of the same person. In some instances, the image of an anonymous individual is compared to images of identified persons in a database, and it is believed that the anonymous individual is in the database (closed-set identification), and in others, it is not known whether the individual is in the database (open-set identification). The latter is used, for example, in comparing an individual against a terrorist watchlist.

AI can also create databases or datasets using data scraped from social media platforms and millions of other websites and can include up to billions of images.

Facial images on video footage can also be extracted and compared against images in a database to identify whether the person in the video is in the database of images (e.g. on the watchlist). Such systems are referred to as Live Facial Recognition Technology (LFRT). The quality of the facial images extracted from video cameras cannot be controlled, and therefore, LFRT is more likely to result in false matches than images taken in a controlled environment, such as a border crossing point or in a police station.[107]

Multiple stakeholders including human rights mechanisms have expressed concerns with respect to the use of facial recognition technologies noting that such technologies have demonstrably shown "gender and racial bias leading to less reliable results when identifying women and persons with darker skin tones".[108] At the same time, the nature and seriousness of concerns depend on the different uses of such technologies. A particular concern was the use of remote real-time, or live, facial recognition increasingly deployed by authorities across the globe for identification purposes.[109] While there are real benefits to using such facial recognition systems for public safety and security, their pervasiveness and intrusiveness, as well as their susceptibility to error, give rise to a number of human rights concerns, with a particular risk of negative impact on the rights to privacy and non-discrimination.

105 Facial recognition technology is also used to extract information about an individual's characteristics. This is sometimes referred to as 'face analysis'. It can, therefore, also be used for profiling individuals, which involves categorising individuals based on their personal characteristics. Characteristics commonly predicted from facial images are sex, age and ethnic origin. Categorisation means that the technology is not used to identify or match individuals, but only characteristics of individuals, which do not necessarily allow for identification. Facial recognition technology can also be used to infer emotions. The serious fundamental rights implications of the categorisation of individuals based on facial images is beyond the scope of this guide.

106 European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in the context of Law Enforcement, Section 3.1. <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

107 European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Considerations in the context of Law Enforcement, Section 3.2. <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf>

108 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 25.

109 The Report of the High Commissioner of Human Rights, the Right to Privacy in the Digital Age, A/HRC/48/31. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement. See also EDPB, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' (12 May 2022), [103]-[104]

In contrast to fingerprints and DNA analysis, for example, there are substantial concerns about the accuracy of facial recognition not only generally but with respect to group characteristics. The general perception of technology is that it is inherently neutral and objective. In fact, technology reflects the values and interests of those who influence its design and use, meaning that it can shaped by the same structures of inequality that operate in society. For example, a 2019 review of 189 facial recognition algorithms from 99 developers around the world found that many of the algorithms were 10 to 100 times more likely to inaccurately identify a photograph of a black or East Asian face, compared with a white one. In searching a database to find a given face, most of them picked incorrect images among black women at significantly higher rates than they did among other demographics.[110] Errors have resulted in false positives, meaning cases in which individuals are singled out and subjected to further scrutiny on the erroneous prediction that they constitute a risk, and false negatives in which individuals who pose a real risk in the context of law enforcement or border management operations are not identified as such by the system.[111] In 2019 in the United States, a facial recognition system misidentified a university student as a terrorist suspect in Sri Lanka's Easter church bombings. Although the police later issued a statement correcting the error, the victim received death threats and faced additional police scrutiny.[112]

As with other surveillance technologies marketed for use to combat terrorism and other serious crime, facial recognition capabilities have at times been used to target minorities, journalists, human rights defenders, journalists, members of political opposition groups, and dissidents.[113] State authorities across the globe have used facial recognition technologies to monitor protests, including peaceful protests, including to track and identify their participants.

In one Member State (the United States), six federal agencies used facial recognition software to identify protesters who demonstrated following an especially grave incident of police brutality,[114] an incident that has also drawn condemnations from UN human rights mechanisms and entities. In another Member State (China), national authorities adopted a programme mandating the collection of extensive biometric data, including facial data, DNA samples and iris scans, to monitor the movements of a particular minority ethnic group. [115] It is able to do so based on common biometric features associated with this group.[116] In yet another Member State (Israel), the authorities use highly sophisticated facial recognition technologies to monitor the activities of a distinct population in an area under its control.[117] As noted above, the prohibition against discrimination in international human rights law is absolute.

The use of facial recognition must be regulated by law in the context of a domestic legal framework consistent with international human rights norms and standards that includes adequate privacy and data protection safeguards. Considering the "high risk associated with the use of biometric tools, due to the sensitive character of biometric data and the potential for exploitation and abuse," conducting comprehensive human rights risk assessments has been advanced as a good practice.[118] In this respect, the mandate of the Special Rapporteur on counter-terrorism and human rights recommended that such risk assessments "examine implications on the right to privacy of data subjects and

110 Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance: Racial discrimination and emerging digital technologies, A/HRC/44/57, para. 12. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/151/06/PDF/G2015106.pdf?OpenElement>

111 European Union Agency for Fundamental Rights, Preventing Unlawful Profiling today and in the future: a guide, p. 22. See also, European Parliamentary Research Service, Regulating Facial Recognition in the European Union, p. 7.< https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf>

112 See Algorithmic Justice League at <https://www.ajl.org/facial-recognition-technology>

113 Report of United Nations High Commissioner for Human Rights. Terrorism and Human Rights, A/HRC/50/49, para. 27.< https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/340/13/PDF/G2234013.pdf?OpenElement>

114 https://thehill.com/policy/technology/560805-watchdog-6-federal-agencies-used-facial-recognition-software-to-id-george/

115 See, e.g. OL CHN 18/2019.

116 Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance: Racial discrimination and emerging digital technologies, A/HRC/44/57, para. 39.< https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/151/06/PDF/G2015106.pdf?OpenElement>

117 See, Washington Post, Israel escalates surveillance of Palestinians with facial recognition program in the West Bank, November 8, 2021.

118 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 42.

incidental effects on third parties, and tackle compliance with recognized data protection principles."[119] The Council of Europe Guidelines on Facial Recognition note that the level of intrusiveness of relevant technology and their impact on human rights will vary "according to the particular situation of their uses and there will be cases where domestic law will strictly limit it, or even completely prohibit it".[120] It further notes that the use of live facial recognition technologies in "uncontrolled environments"(such as places freely accessible to individuals, where they can also pass through, including public and quasi-public spaces such as shopping malls, hospitals, or schools)"should be subject to a democratic debate on its use and the possibility of a moratorium pending complete analysis" due to the level of intrusiveness and the risk of adverse impact on human rights.[121]

Against this background, live technologies in uncontrolled environments should only be deployed pursuant to such democratic debate that duly considers their impact, including from a human rights point of view, and subject to authorities demonstrating that their use is necessary and proportionate under the circumstances.[122] In this context, authorities should also consider the vulnerability of data subjects that may be impacted by the measures and ways to effectively mitigate relevant risks.

As facial recognition technologies can be used without the consent or even knowledge of data subjects, the transparency and fairness of the processing are of the utmost importance. At a minimum, legislation on facial recognition or the collection, retention, processing, transfer or other use of similar biometric data should specify the following:

- That data be obtained and processed fairly and lawfully;
- That data be stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- That data collected be adequate, relevant and not excessive in relation to the purposes for which they are stored;
- That data be accurate and, where necessary, kept up to date;
- That data be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored, meaning that legislation must include guidelines on the retention, deletion or de-identification of the data; and
- Should specify whether and to what extent facial data can be transmitted to third parties.

States should also provide information regarding the contact points available for individuals to ask questions about the collection, retention, use and sharing of their biometric data, including data generated in relation to facial recognition technologies, and security measures must be taken to safeguard the security of biometric systems and prevent loss of or unauthorized access to data.

As facial recognition is based on the processing of personal data, data subjects should have: the right to information, the right of access, the right to obtain knowledge of the underlying reasoning for the collection and/or retention of data, the right to object and the right to rectification. In case personal or sensitive data has been collected or used in contravention with international human rights law, data subjects should be provided with effective remedy.

119 Ibid.

120 Council of Europe, Consultative Committee of Convention 108 on Data Protection, Guidelines on Facial Recognition. <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>

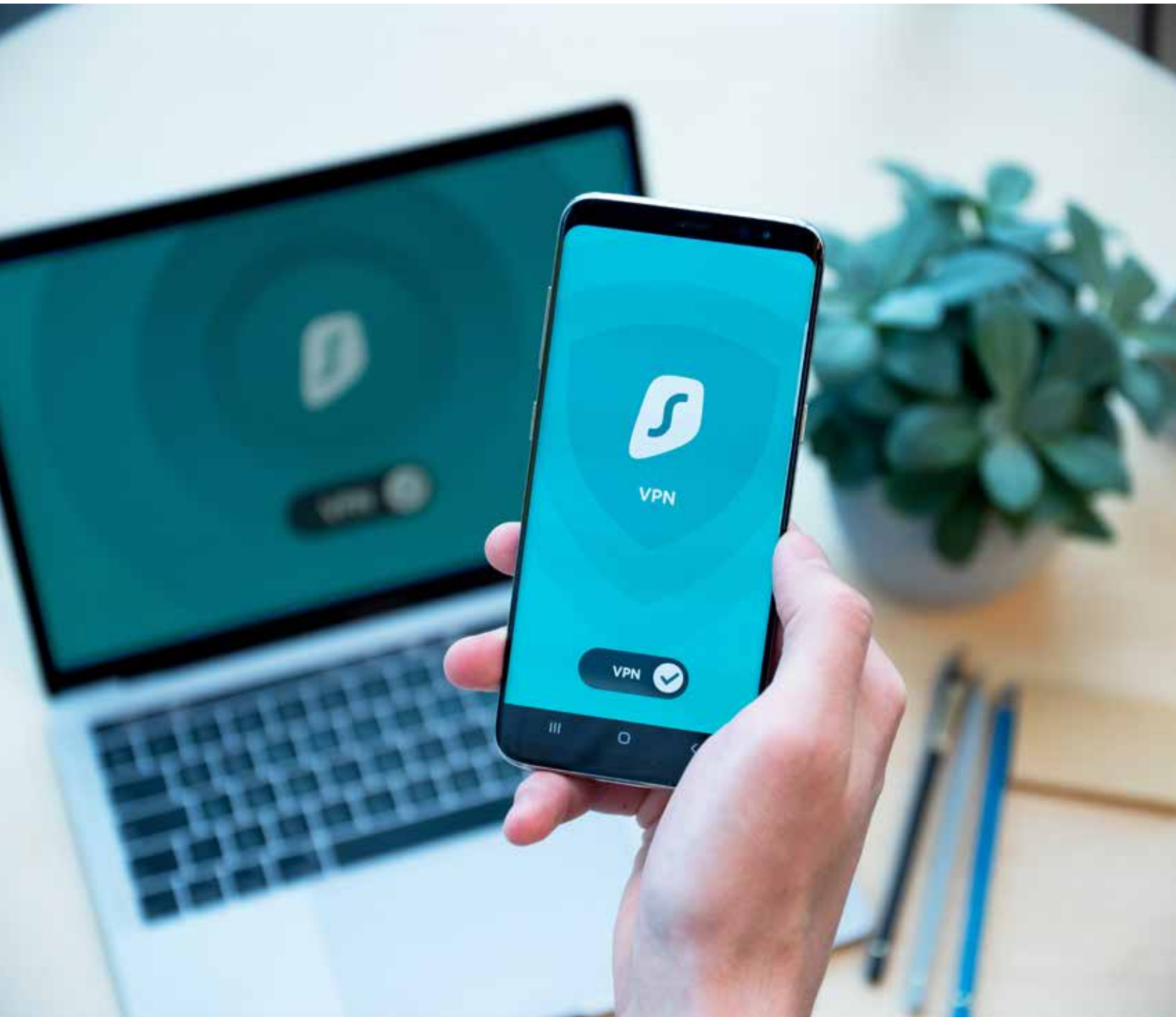
121 bid.

122 In this respect, see alsoEDPB, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement' (12 May 2022), [103]-[104]

Finally, as consistently observed by human rights mechanisms, including the Special Rapporteur on counter-terrorism and human rights, cross-border data-sharing, including practices relating to the sharing of biometric data raise concerns from a human rights perspective, with the Special Rapporteur having referred to such arrangements as a "black box of international law practice, with little information available on whether and what type of biometric data are exchanged, and, more practically, on the content of data-sharing agreements".[123] For this reason, the mandate of the Special Rapporteur has highlighted that data-sharing practices must be driven by the principle of accountability and subject to comprehensive independent oversight.[124]

123 A/HRC/ 52/39, para. 26.

124 K. Huszti-Orbán and F. Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' (2020), https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/biometricsreport.pdf, p. 43.



[VIII] Unlawful Obtained Evidence

8.1 Unlawfully Obtained Evidence

In determining how to conduct surveillance activities using new technologies LEAs must bear in mind that obtaining evidence unlawfully undermines the integrity of legal proceedings against those suspected or accused of criminal activity. International human rights law guarantees the right to a fair hearing and while it is beyond its scope lay down granular rules on the admissibility of evidence (this being a matter for domestic law), it does provide guidance when it comes to ensuring the fairness of proceedings more broadly and the role that evidence and admissibility rules play in this respect. Importantly, the use of evidence obtained through torture or cruel, inhuman or degrading treatment is incompatible with international human rights law including the right to a fair trial. When it comes to other unlawful evidence, different jurisdictions take different approaches with some automatically excluding such evidence from use in criminal justice processes. In others, such evidence is not, a priori, inadmissible, but the manner and circumstances in which the evidence was obtained, as well as its reliability and impact on the integrity of proceedings, will determine its admissibility. For example, the European Court of Human Rights has held that the question is whether the proceedings as a whole, including the way in which evidence was obtained, were fair.

[IX]

Algorithmic Profiling and Non-Discrimination

9.1 Algorithmic Profiling and Non-Discrimination

Technological developments have triggered an increased use of profiling in a wide range of contexts, including law enforcement, border control and security. Profiling is commonly used by law enforcement officers and border guards to prevent and investigate criminal offences. Such practices are sued to "establish correlations between certain characteristics and particular outcome or behaviour" [125] which may not be true fall all individuals falling within the respective 'profile'. Profiling is used 1) to identify known individuals based on intelligence concerning a specific individual ('specific intelligence-led policing'), and 2) as a predictive method to identify 'unknown' individuals who may be of interest to law enforcement and border management authorities ('predictive policing').[126]

While definitions of profiling vary, the practice has been described as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[127] In recent years, algorithmic profiling has increasingly been used based on data stored in different databases and information management systems.

For profiling and related practices to be consistent with the rule of law and international human rights norms and standards, they must have a sufficiently foreseeable and accessible legal basis, grounded in objective and reasonable justifications[128] and conducted pursuant to a process that contains adequate safeguards against abuse and is subject to meaningful oversight. Profiling may engage a range of human rights considerations, such as those related to privacy and data protection, due process and fair trial, etc. Importantly, profiling practices must be designed and conducted in a manner compliant with the right to non-discrimination. As such, profiling that primarily or significantly relies on protected characteristics such as gender, race, ethnicity, religion, age, etc. or that results in direct or indirect discrimination against persons on the basis of such characteristics contravenes the prohibition of non-discrimination and shall not be permitted.

125 European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide (2018), p. 16.

126 Ibid, pp. 16 and 18.

127 See e.g. Directive (EU) 2016/680.

128 An objective and reasonable justification requires that the measure pursue a legitimate aim and a relationship of necessity and proportionality "between the means employed and the aim sought to be realized". See, e.g. European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide (2018), p. 23; European Court of Human Rights, Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention, available at https://www.echr.coe.int/documents/d/echr/Guide_Art_14_Art_1_Protocol_12_ENG. See also Human Rights Committee, general comment No. 31 2004, para. 6, and *Genero v. Italy*, para. 7.6; and Committee on Economic, Social and Cultural Rights, general comment No. 20 (2009), para. 13, and *Trujillo Calero v. Ecuador*, para. 19.5. See also Committee on the Elimination of Racial Discrimination, General Recommendation No. 32 (2009), para. 8.

In counter-terrorism contexts, concerns have been raised about the use of racial or ethnic profiling. The United Nations Committee on the Elimination of Racial Discrimination has described racial profiling as an act(a) committed by law enforcement authorities; (b) [...] not motivated by objective criteria or reasonable justification; (c) [...] based on grounds of race, colour, descent, national or ethnic origin or their intersection with other relevant grounds, such as religion, sex or gender, sexual orientation and gender identity, disability and age, migration status, or work or other status; (d) [...] used in specific contexts, such as controlling immigration and combating criminal activity, terrorism or other activities that allegedly violate or may result in the violation of the law". [129] The mandate of the Special Rapporteur on counter-terrorism and human rights noted that law enforcement practices using "broad profiles that reflect unexamined generalizations," may constitute disproportionate interferences with human rights. The Special Rapporteur further stressed that "profiling based on stereotypical assumptions that persons of a certain "race", national or ethnic origin or religion are particularly likely to commit crime may lead to practices that are incompatible with the principle of non-discrimination" and expressed grave concern about the adoption of counter-terrorism practices that are "based on terrorist profiles that include characteristics such as a person's presumed "race", ethnicity, national origin or religion."[130] He highlighted that such practices are not "unsuitable and ineffective means of identifying potential terrorists, but they also entail considerable negative consequences that may render these measures counterproductive in the fight against terrorism".[131]

The Committee on the Elimination of Racial Discrimination noted that racial profiling was linked to "stereotypes and biases, which can be conscious or unconscious, and individual or institutional and structural" and that stereotyping violated international human rights law when such stereotypical assumptions "are put into practice to undermine the enjoyment of human rights".[132] Other studies have shown that profiling on discriminatory grounds is not only inaccurate but otherwise ineffective. For example, terrorist groups have proven their ability to circumvent established profiles by recruiting individuals who are less likely to get searched under predictive profiles. Additionally, a study conducted by the Organization for Security and Cooperation in Europe concluded that extensive identification controls carried out by some OSCE Member States at mosques, as well as ethnically based data-mining exercises and stop-and-search programmes, did not result in any counter-terrorism convictions.[133]

129 Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by aw enforcement officials, para. 13. The Committee described ethnic profiling as "the use by the police, with no objective and reasonable justification, of criteria such as race, colour, language, religion, nationality or national or ethnic origin, for control, surveillance, or investigation activities." See Ibid., para. 13. See also, European Commission against Racism and Intolerance, General Policy Recommendation No 11 on Combating Racism and Racial Discrimination in Policing, CRI (2007)39, 29 June 2007, page 4. See also, Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by law enforcement officials, para. 13: See also, Inter-American Commission on Human Rights, "The situation of people of African descent in the Americas" (2011), para. 143: as a tactic adopted for supposed reasons of public safety and protection motivated by stereotypes based on race, colour, ethnicity, language, descent, religion, nationality or place of birth, or a combination of these factors, rather than on objective suspicions, which tends to single out individuals or groups in a discriminatory way based on the erroneous assumption that people with such characteristics are prone to engage in specific types of crimes. The Arab Human Rights Committee has submitted that racial profiling can be defined as the use by law enforcement agents of generalizations or stereotypes related to presumed race, colour, descent, nationality, place of birth, or national or ethnic origin – rather than objective evidence or individual behaviour – as a basis for identifying a particular individual as being, or having been, engaged in a criminal activity, resulting in discriminatory decision-making (see General Comment 36, para. 15).

130 A/HRC/4/26, para.34. See also A/HRC/29/46, para. 2.

131 A/HRC/4/26, para. 83.

132 Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by law enforcement officials, para. 20.

133 OSCE Office for Democratic Institutions and Human Rights, Report on the Expert Meeting on Security, Radicalization and the Prevention of Terrorism", 28–29 July 2008, para. 25. <www.osce.org/odihr/34379>

The Committee on the Elimination of Racial Discrimination further observed that while the use of AI can in certain circumstances contribute to more effective decision-making, it comes with a real risk of algorithmic bias in particular in the context of law enforcement.[134] Even where stereotypes may reflect some statistical truth, profiling is problematic if individuals are profiled as members of a group rather than based on individual characteristics and behaviour. As such, algorithmic profiling may raise serious concerns, among others, as it can reproduce and reinforce biases and aggravate or lead to discriminatory practices. Given the opacity of algorithmic analytics and decision-making, in particular, when artificial intelligence methods are employed, discriminatory outcomes are often less obvious and more difficult to detect than those of human decisions, and thus more difficult to contest.[135] This has potentially serious consequences on the rights of the victims. For this reason, it has also been recommended that national human rights structures, including equality bodies, as well as independent police oversight authorities play an active role "in detecting and mitigating the risks associated with the use of algorithms in the criminal justice systems".[136]

With the use of machine-learning algorithms in the criminal justice systems becoming increasingly common in the field of "predictive" policing, algorithmic profiling techniques are increasingly resorted to Its uses include 1) predicting where crimes may occur and how best to allocate police resources; assessing the risk of reoffending in the context of criminal justice processes including in relation to decisions on remand in custody, sentencing and parole. While predictive methods should focus on behaviour, in practice, the emphasis is "often not (or not only) on behaviour, but on visible physical characteristics, such as age, gender or ethnicity."[137] The prediction of criminal behaviour in particular should not be only based on statistics generated by algorithms but be corroborated by other indicia and facts.

A 2016 study of the latter technology in the United States found that it made mistakes roughly at the same rate for both White and Black individuals, but was far more likely to produce false positives (a mistaken `high risk´ prediction) for Blacks and more likely to produce false negatives for Whites.[138]

Particular risks emerge when algorithmic profiling is used to determine the likelihood of criminal activity either in certain localities, or by certain groups or individuals. For example, historical arrest data about a neighbourhood may reflect racially biased policing practices. If fed into a predictive policing model, the use of these data poses a risk of steering future predictions in the same, biased direction, leading to over-policing of the same neighbourhood, which in turn may lead to more arrests in that neighbourhood, creating a dangerous feedback loop.[139] At the same time, in situations when members of a particular ethnic group or religious community may be under threat, it is not discriminatory or disproportionate to allocate the necessary law enforcement resources to the protection of that group.

134 Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by law enforcement officials, para. 12.

135 Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by law enforcement officials, para. 32. <https://digitallibrary.un.org/record/3897913>

136 Council of Europe, Commissioner for Human Rights, Ethnic profiling: a persistent practice in Europe. <https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe>

137 European Union Agency for Fundamental Rights, Preventing unlawful profiling today and in the future: a guide (2018), p. 18.

138 Council of Europe, Commissioner for Human Rights, Ethnic profiling: a persistent practice in Europe. <https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe>

139 Committee on the Elimination of Racial Discrimination, General Recommendation 36 on preventing and combating racial profiling by law enforcement officials, para. 33. <https://digitallibrary.un.org/record/3897913>

In addition to being unlawful, discrimination in the implementation of responses to terrorism risks hampering the effectiveness of counter-terrorism efforts. Discriminatory measures risk alienating groups and creating or exacerbating grievances that could be conducive to the rise of the terrorist threat. Profiling can generate resentment among the communities particularly affected and reduce trust in the police and border management authorities. This in turn can undermine the effectiveness of methods that rely on public cooperation.

The use of excessively broad criteria can also lead to a significant number of unhelpful 'false positives', meaning that persons are wrongly matched with a certain risk profile. Some of these 'false positives' might also be discriminatory in nature. For instance, as the European Union Agency for Fundamental Rights has noted, if a risk profile concerning the risk of irregular migration is based on the combination of a certain nationality and occupational group, it may result in targeting an ethnic group or nationality which in a certain country typically works in a particular economic sector, such as construction or agriculture. In other cases, a broad definition of the criterion 'past criminal conviction' would lead to LGBTI+ individuals being "required to report criminal records associated with certain sexual conduct criminalized" by some countries.[140]

140 European Union Agency for Fundamental Rights, Preventing Unlawful Profiling today and in the future: a guide, pp. 27-28. <https://fra.europa.eu/en/publication/2018/preventing-unlawful-profiling-today-and-future-guide> See also, Council of Europe, Commissioner for Human Rights, Ethnic profiling: a persistent practice in Europe, pp. 117-118. < https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe>

[X]

Social Media, Internet, Freedom of Expression/Association & Incitement

10.1 General Issues

New technologies have played an important role in enhancing the public's access to seek, receive and impart information. Such technologies and tools can also provide a platform for persons and groups that are less included in debates of public interest, such as women or individuals belonging to marginalized or underrepresented groups. They can also create and strengthen social bonds, increase access to healthcare, education, and social welfare tools, facilitate knowledge designed to promote sustainable development, allow marginalized communities to build networks, and foster more open, inclusive and diverse public spheres.[141]

At the same time, ICTs, the Internet including social media platforms have at times also been co-opted by terrorist actors for and utilized among others to promote and support terrorist acts, by disseminating propaganda, online recruitment, radicalization and incitement to terrorism, for financing as well as for the execution of attacks, including by disseminating technical instructions on how to obtain weapons and carry out violent acts.

In 2013, Al Shabaab live tweeted its attack on the Westgate Mall in Nairobi.[142] It has also used the internet to solicit donations from the Somali diaspora and others, in one effort raising over $40,000.[143] The account of an Al Qaeda affiliated individual posted a photo of a drone on a social media site and wrote: "Russian Surveillance plane falls down in Lattakia [Syria] region near the Sunni Fighters! It could perhaps be a great development if the fighters reverse engineer it!"[144] In 2016, a Telegram channel titled "Islamic State Scientists & Engineers" was launched. Among its public goals: "i) collect as much caliphate scientists & engineers as possible from around the world & introduce them to each other; and ii) use them to create a powerful worldwide industrial network to support the military industry in the Islamic State."[145] On October 16, 2014, the leading English-language ISIL Twitter account tweeted a link to a PDF file titled "The Beginner's Guide to Multicopters," which provided instruction on how to build entry-level

141 Council of Europe, Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression. <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a61729>

142 See, <https://www.cbc.ca/news/world/kenya-attack-why-al-shabaab-live-tweeted-the-assault-1.1865566>

143 2010 Report of the Monitoring Group on Somalia pursuant to Security Council resolution 1853 (2008), para. 92. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/246/89/PDF/N1024689.pdf?OpenElement>

144 Middle East Media Research Institute, (MEMRI), A decade of Jihadi Organizations' Use of Drones, 1027. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>

145 Middle East Media Research Institute, (MEMRI), A decade of Jihadi Organizations' Use of Drones, 1027. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>

multi-rotor drones.[146] Similarly, a group of pro-Islamic State technicians used Telegram to discuss how common engine parts might be adapted for use in missiles or in military-style attack drones.[147]A Taliban online magazine called on "our skillful Muslim brothers who are engineers and scientists to come forward and try their best in figuring out how to break the link between drone and GPS. Experiment in whichever part of the world you live and if it's successful, make a complete video demonstration of the process, upload it on the web and make it password protected. Then send that link and password to us. Or simply make a good… PowerPoint [presentation] and send it to us. Even if you have made good progress in the experiment but encountered some complication in it then send it to us, maybe we can suggest something useful to you".[148]

the limits of freedom of expression under international human rights law, the European Court of Human Rights has held that "[t]olerance and respect for the equal dignity of all human beings constitute the foundations of a democratic, pluralistic society. That being so, as a matter of principle it may be considered necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance …, provided that any 'formalities', 'conditions', 'restrictions' or 'penalties' imposed are proportionate to the legitimate aim pursued".[149]

While, restrictions on freedom of expression and other relevant rights such as the right to freedom of association are necessary as part of legitimate counter-terrorism efforts, some jurisdictions have imposed undue restrictions on online content or services, among others by shutting down internet services or selectively blocking access to online resources and sites,. In some jurisdictions, journalists, the political opposition, human rights defenders, anti-corruption activists, and other individuals faced harassment or have been targeted, including with criminal justice measures, merely for exercising their freedom of expression online. In 2018, the United Nations High Commissioner for Human Rights observed that "the Internet is increasingly a space of threat for human rights defenders".[150]

10.2 Open-Source Intelligence

Modern technologies have vastly augmented the information available to LEAs and intelligence agencies through open-source investigative techniques (OSINT). Indeed, OSINT is a critical component of the modern investigator or analyst's toolkit both for the prevention of terrorist acts and for the prosecution of individuals or groups accused of such acts. This is particularly true when OSINT is used in complement with other information collection activities. Using the growing number of on-line data bases, and the internet more generally, OSINT researchers can search media sites, social media accounts, maps, satellite imagery, videos, photos, and other digital content from their computer terminals to identify terrorist propaganda, and information on terrorist operations, techniques, and leaders.

As with all investigations, the use of OSINT should serve a legitimate aim, be proportionate to that aim and non-discriminatory. Such techniques should not be used to collect information for purposes of monitoring, surveilling, harassing, or intimidating individuals pursuing legitimate activities. Authorities should also be mindful of the challenges connected to the use of OSINT such as the volume and reliability of the available data; limitations of and safeguards needed to accompany automated analysis; and the personal or sensitive nature of information.[151]

146 Middle East Media Research Institute, (MEMRI), A decade of Jihadi Organizations' Use of Drones, 1027.<https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>

147 Middle East Media Research Institute, (MEMRI), A decade of Jihadi Organizations' Use of Drones, 1027. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>

148 Middle East Media Research Institute, (MEMRI), A decade of Jihadi Organizations' Use of Drones, 1027. <https://www.memri.org/reports/decade-jihadi-organizations-use-drones-%E2%80%93-early-experiments-hizbullah-hamas-and-al-qaeda>

149 European Court of Human Rights, *Erbekan v. Turkey*, Judgment of 6 July 2006, § 56.

150 https://www.ohchr.org/en/statements/2018/11/human-rights-new-era

151 See, e.g., https://responsibledata.io/2016/11/14/responsible-data-open-source-intelligence/

10.3 Online Terrorist Content Including Incitement to Terrorism

Security Council resolution 1624 (2005) calls on States to prohibit by law incitement to commit a terrorist act or acts. However, given that States have justified limitations on all types of speech in the name of combatting incitement to commit terrorist acts, it is critical that States take great care in implementing the resolution. As addressed earlier, the mandate of the Special Rapporteur on counter-terrorism and human rights has proposed a model definition of incitement to terrorism.[152] The mandate, together with United Nations human rights mechanisms and other stakeholders, has stressed the need for incitement of terrorism as well as other offences criminalizing the advocacy of terrorism, including 'glorification', 'apology', 'praise' or 'justification' of terrorism to have precise definitions to avoid over-broad scope or attaching criminal sanctions to conduct that falls short of incitement to terrorism or advocacy of national, racial or religious hatred constituting incitement to violence.[153]

Regulation (EU) 2021/784 defines terrorist content as content which:[154]

- Solicits someone to commit or to contribute to terrorist offences, or to participate in activities of a terrorist group,
- Incites or advocates terrorist offences, such as by glorification of terrorist acts; and
- Provides instruction on how to conduct attacks.

Addressing terrorist content including incitement to commit terrorist acts implies interference with and limitations of human rights such as freedom of expression. Content can be removed or restricted and freedom of expression limited if such measures are necessary for respect of the rights or reputations of others; or for the protection of national security or of public order (order public), or of public health or morals. Furthermore, States are required to prohibit advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence in line with article 20 of the International Covenant on Civil and Political Rights. In implementing their obligations under article 20 (2) of the ICCPR, Member States are invited to consider the guidance contained in the Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence,[155] in particular the six-part threshold test set out therein. This test considers the following elements when assessing speech that may amount to criminal advocacy of hatred: (1) context; (2) speaker; (3) intent; (4) content and form; (5) extent of the speech act; and (6) likelihood, including imminence.[156]

152 See Section V.

153 Article 20, ICCPR.

154 Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of content online, Article 2 (7): Terrorist content means…:

(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3 (1) of EU Directive 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;

(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;

(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;

(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541. < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32021R0784>

155 A/HRC/22/17/Add.4.

156 A/HRC/22/17/Add.4, para. 29.

States have a variety of tools at their disposal to address terrorist content including: i) request that service providers remove the content in question; ii) impose civil penalties on those responsible; and, iii) prosecute the individual or group responsible.

10.3.1 Content Removal

As addressed earlier in this Guide, Member States have an obligation under international law to take measures to prevent and counter terrorists' acts. This obligation is also connected to the due diligence obligation under human rights law that States take appropriate measures to protect persons within their jurisdiction from undue interference with their human rights by third parties, including terrorist actors and, if prevention fails, ensure accountability for such conduct. As such, it is the primary obligation of Member States to both take measures to ensure that online content is regulated in line with international human rights law, including that corporate actors conduct their relevant activities in a manner that is respectful of the human rights of persons within the respective State's jurisdiction.

Whereas a number of Member States and regional organizations have adopted legislation on addressing online content, including content of a terrorist nature, Member States have also required tech companies that provide a platform for and curate third-party content to monitor and police, on behalf of the State, online content that is generated or disseminated by users. In some cases, relevant legal and policy frameworks did not comprehensively address human rights considerations nor did they provide guidance to corporate actors on ensuring respect for human rights.

While Member States have the primary responsibility when it comes to ensuring the promotion and protection of human rights for all persons within their jurisdiction, the growing role of corporate actors and their increased impact on the enjoyment of human rights is addressed by the UN Guiding Principles on Business and Human Rights which provide an authoritative global standard for preventing and addressing adverse human rights impacts linked to business activity.[157] In line with the Guiding Principles, business enterprises have a set of due diligence responsibilities requiring them to conduct risk assessments examining actual and potential human rights impacts, both direct and indirect, of their operations. Such risk assessments will enable the company to develop and implement mitigation measures if and when necessary. Companies should set up internal accountability mechanisms for the implementation of human rights policies and have processes in place that enable the remediation of adverse human rights impacts that the company caused or contributed to. They should communicate externally on the measures they take to address human rights impacts linked to their operations, particularly when concerns are raised by or on behalf of affected stakeholders, through regular transparency reporting.

Successfully tackling the use of Internet for terrorist purposes requires meaningful cooperation between public authorities and a broad range of private actors, including tech companies. The intersection of State and corporate roles and responsibilities in the digital age remains a challenge both for Member States and corporate actors, one that is particularly discernable in the counter-terrorism context.

Meta has established an independent body, comprised of academics and other experts on technology and freedom of speech issues, to review, inter alia, Facebook and Instagram responses to content removal requests and to advise on policy issues. Its decisions contribute to broader discussions on ways to ensure respect for human rights including freedom of expression in the online context.

157 While the Guiding Principles have been endorsed by the Human Rights Council (resolution 17/4), they are not formally legally binding. This means that *the responsibilities entailed in the* Guiding Principles *are not as such legally enforceable without them being transposed in domestic legislation. At the same time*, the Guiding Principles represent an important step towards matching the impact of businesses on human rights with corresponding levels of corporate responsibility. They also represent the direction of normative development at the international and domestic level and they are being recognized, accepted and implemented by a growing number of business enterprises, including tech companies. In this sense see also OL OTH 46/ 2018; OL OTH 71/2018.

BOX 13. META OVERSIGHT BOARD CASE-1

In 2021, a Facebook user shared a post by the verified Al Jazeera Arabic page consisting of text in Arabic and a photo. The photo portrayed two men in camouflage fatigues with faces covered wearing headbands with the insignia of a group designated as dangerous under Facebook's Dangerous Organizations and Individuals Community Standard.

The text stated: "The resistance leadership in the common room gives the occupation a respite until 18:00 to withdraw its soldiers from (the named) Mosque...Otherwise, he who warns is excused." — Group military spokesman.

The Oversight Board affirmed Facebook's decision to restore the content it had initially removed. In doing so, it observed the post did not contain praise, support or content of a Dangerous Organization. It was merely a replication of a news item on a legitimate news outlet on a matter of urgent public concern. Additionally, Facebook told the Board that it had not received a valid legal request from a government authority to remove the content meaning that no government authority was called upon to justify a removal request.

BOX 14. META OVERSIGHT BOARD CASE-2

In another decision, the Oversight Board overturned a Facebook decision to remove an Instagram post encouraging people to discuss the solitary confinement of the leader of a dangerous organization. Both the organization and its leader had been designated as "Dangerous Entities" in accordance with Facebook policy.

An Instagram user had posted a picture of the leader with the words "y'all ready for this conversation." The user encouraged readers to engage in a conversation about the leader's imprisonment and the inhumane nature of solitary confinement.

Following its initial removal decision, Facebook informed the Board that it was updating its policies to allow users to discuss the human rights of designated dangerous individuals. The Oversight Board overturned Facebook's initial decision to remove the content and instructed Facebook to specify in updated policy guidance "the real world harms the policy seeks to prevent and disrupt when a "Voice" is suppressed and add a clear explanation of what "support" to a Dangerous Individual or Organization excludes".

BOX 15. META OVERSIGHT BOARD CASE-3

In 2022, a newspaper reported on its Facebook page that the spokesman of a dangerous organization had announced that schools for women and girls in the area under the organization's control would soon re-open.

Meta found that the post violated the Dangerous Individuals and Organizations Policy which prohibits "praise" of entities deemed to "engage in serious offline harms".

Meta later reversed the removal decision concluding that its Community Standard permits content that "reports on" Dangerous Organizations. The Oversight Board overturned Facebook's initial decision to remove the content noting that the right to receive and impart information, including on terrorist groups, is particularly important in times of conflict and crisis, including where terrorist groups exercise control of a country.

10.3.2 **Imposition of Civil Penalties**

Any civil penalties imposed on individuals or organizations inciting terrorist acts must be provided by law and comply with the principles of necessity and proportionality, and subject to independent administrative or judicial oversight and appeal.

BOX 16. **The IACtHR* Finds that the Imposition of Civil Penalties Violates Freedom of Expression**

In a case before the Inter-American Court of Human Rights, the Court reviewed a State's judicial decision "disqualifying" individuals convicted of terrorist acts for 15 years from "exploiting a social communication medium or from being a director or administrator of one, or from performing functions related to the emission and diffusion of opinions and information".

The Court held that the punishment violated the principle of proportionality, particularly as the accused were leaders of a marginalized community, whose human rights had been consistently violated, and the punishment would restrict their ability to take part in the diffusion of opinions, ideas and information, which in turn would restrict their right to freedom of thought and expression in the exercise of their functions as leaders or representatives of their communities.

In addition, the Court held that the State's improper application of counter-terrorism legislation might have an intimidating and inhibiting effect on the exercise of freedom of expression on other members of the marginalized community, referring to the intimidating effect on the exercise of freedom of expression that may result from the fear of being subject to a civil or criminal sanction that is unnecessary or disproportionate in a democratic society, and that may lead to the self-censorship of the person on whom the punishment is imposed, and on other members of society. The Court concluded that the way in which the Counter-terrorism Act was applied to members of the marginalized community might instill a reasonable fear in other members of the community involved in social protest seeking recognition of territorial rights.

Norín Catrimán v. Chile, paras. 374-376.
* Inter-American Court of Human Rights

BOX 17. The ECtHR* Finds that the Imposition of Civil Penalties does not Violate Freedom of Expression

The Court reviewed a national judicial decision to fine a broadcaster within a Member State approximately 671,000 euros for having promoted a group that had been designated as a terrorist organization by the EU, Canada, USA, Australia, and the United Kingdom. The national court rejected a request to withdraw the broadcaster's license.

The ECtHR considered that the domestic courts carefully assessed the evidence before them and conducted a balancing exercise which took the applicant company's right to freedom of expression into account. Evidence before the national courts included that when covering the armed conflict between a third Member State and the designated group, the broadcast had primarily relied on information obtained from the group's supporters without the involvement of any other sources. In a number of programmes, the group's leaders were heard explaining the organisation's views and inciting revolt, which the TV host listened passively. The broadcaster made no effort to distance itself from the incitements or to include other views, for example by posing critical questions. The biased coverage of the group's activities, incitement and messages was reinforced by the language of the TV host when for example, he referred to the arrest of the group's leader as an international plot. Coverage also included referring to deceased members of the groups as "heroes" and "martyrs" and mentioning concrete actions carried out by the group which resulted in casualties among the police and military forces of the third State. The national courts found that the biased broadcasting together with "repetitive incitement to participate in the fights, and actions, incitement to join the organization/guerilla" amounted to propaganda on the behalf of the terrorist group rather than mere sympathy for the group. The national court also found that the broadcaster had been financed to a significant extent by the terrorist organization. The national courts also observed that other programmes broadcast by the company about the general situation of a marginalized group associated with the terrorist group, including on their language, culture and politics. The ECtHR found that taking account of (1) the nature of the impugned programmes, which included incitement to violence and support for terrorist activity, (2) the fact that the views expressed therein were disseminated to a wide audience through television broadcasting and, (3) that they related directly to an issue which is paramount in modern European society - the prevention of terrorism and terrorist-related expressions advocating the use of violence - the applicant company´s complaint does not attract the protection afforded by the Convention with regard to freedom of expression. Consequently, the ECtHR declared the case inadmissible.

ROJ TV/AS v. Denmark, paras. 9, and 39-49.
*The European Court of Human Rights

10.3.3 Criminal Prosecution

States have an obligation to prohibit and duly address incitement to terrorism and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Such conduct, depending on the concrete circumstances, may warrant criminal justice measures against the perpetrators. At the same time, a number of States have imposed drastic sentences on individuals linked to online content. In one Member State (Iran), authorities executed an individual who administered a popular news channel on Telegram, after he was convicted of inciting protests and being affiliated with foreign intelligence services.[158]

Both the African Court of Human and Peoples' Rights and European Court of Human Rights have reviewed cases imposing penal sanctions and assessed the appropriateness of sentences imposed in criminal cases against human rights standards.

When addressing speech-based offences, it is critical to consider that prosecutions based on expression may have a chilling effect on the way others interpret their right to freedom of expression, usually resulting in self-censorship.

158 See Amnesty International, December 12, 2020: Iran: Execution of journalist Rouhollah Zam a 'deadly blow' to Freedom of Expression.

While some of the impugned expression set out in the boxes below were not made online, the examples and analysis are equally relevant to offline and online expression.

BOX 18. The ECtHR* Finds that Criminal Conviction Violates Freedom of Expression

The case concerned the participation of a former Basque separatist politician in a ceremony to pay tribute to a former member of a terrorist organization and his conviction and sentencing to one year in prison for publicly defending terrorism.

The Court found that although the accused had made statements during a ceremony in memory of a former member of a terrorist organization in a tense political and social context, the content and formulation of the contents showed that he had not intended to incite people to violence or to condone or defend terrorism thus no direct or indirect incitement to violence had been established. On the contrary, the impugned speech at the ceremony had advocated pursuing a democratic means of achieving a specific political objective. Therefore, the restrictions on freedom of expression could not be considered to be "necessary in a democratic society."

Erminia Almandoz v. Spain, paras. 42–50.
*The European Court of Human Rights

BOX 19. The ACHPR* Finds that Criminal Conviction Violates Freedom of Expression

Based on a number of public speeches, the accused, an opposition political leader, was convicted and sentenced to 15 years imprisonment for "aiding and abetting terrorism", "attempted recourse to terrorism…and other forms of violence to destabilize the established authority and violate constitutional principles" and "undermining the internal security of the State, spreading rumours likely to incite the population against political authorities and mount citizens against one another."

The Court reviewed statements made by the accused and concluded that while they might "be offensive" and might discredit the integrity of public officials and institutions of the State, "government institutions and public officials cannot be immune from criticism: and the statements: cannot reasonably be considered as capable of 'inciting strife'…or 'threatening the security of the State."

In the matter of I*ngabire Victoire Umuhoza, V. Rwanda*, paras. 160–161.

BOX 20. The ECtHR* Finds Sentence Imposed for Praise of Terrorism Disproportionate

The accused was a former member of a terrorist group. On a radio show that was recorded and subsequently posted to a website, he characterized the perpetrators of a terrorist attack as "brave" and said that they had "fought bravely." He was convicted of publicly defending an act of terrorism and sentenced to 18 months imprisonment, although ten months of that sentence was suspended.

The Court found that while the applicant's speech had not amounted to a direct incitement to violence, they had conveyed a positive image of the perpetrators of terrorist attacks and the statement had been uttered at a time when French society was still reeling from the deadly 2015 attacks and the level of terrorist threat remained high. However, the Court further found that, in the concrete circumstances of the case, the sentence imposed was disproportionate to the legitimate aim pursued and not necessary in a democratic society.

Rouillan v. France, paras. 60, 69–71, 75–76.
* The European Court of Human Rights

[XI]

Circumvention Technologies

11.1 Circumvention Technologies

While it is indisputable that bad actors use encryption for nefarious ends, there are a multitude of legitimate reasons why individuals may prefer numerous legitimate reasons that individuals or group may choose to use technologies that protect anonymity or evade detection, including use of Virtual Private Network (VPNs), the Dark Web, crypto currencies, or encrypted messaging services.

For example, human rights defenders may resort to the Dark Web when States shut down other service providers or otherwise severely restrict freedom of expression. Law enforcement, human rights defenders, medical practitioners, and journalists may use encrypted messaging services to protect the identity of sources and informants as well as other confidential information such as medical records. Individuals and groups may consider that using peer-to-peer cryptocurrency transactions is a way to circumvent predatory banking practices, or disproportionately onerous financial reporting requirements.

The Office of the United Nations High Commissioner for Human Rights (OHCHR) has warned governments against undermining encryption stating, "[e]ncryption is a key enabler of privacy and security online and is essential for safeguarding rights. In recent years, various Governments have taken actions, which, intentionally or not, risk undermining the security and confidentiality of encrypted communications. This has concerning implications for the enjoyment of the right to privacy and other human rights".[159]

The UN Special Rapporteur on freedom of expression has written that "encryption secures a "zone of privacy" that enables individuals to develop and share opinions through online correspondence and other digital media. Encryption provides individuals the assurance that their "communications are received only by their intended recipients without interference or alteration, and that the communications they receive are equally free from intrusion." In some cases, encryption may also guarantee anonymity: the use of specially designed encryption schemes such as Tor anonymizes metadata (such as the time, date and place of an individual's communications and online activities) and digital identifiers (such as email or IP addresses).[160]

159 See, e.g., A/HRC/51/17, para. 21.

160 A/HRC/38/35, Add. 5, para. 6.

BOX 21.

In Country X, a Telecommunications Regulation Law addresses 'National Security' and 'General Mobilisation.' One article prohibits telecommunications providers and users from using encryption equipment without written permission from the Telecom Regulation Authority, the Armed Forces and National Security Entities.

Principle 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa[161] prohibits Member States from adopting laws that "prohibit or weaken encryption, including backdoors, key escrows and data localization requirements, unless such measures are justifiable and compatible with international human rights law and standards."

The United Nations and regional human rights mechanisms have recommended that States should not adopt, or should revise, laws and policies which involve the following:[162]

- Blanket prohibitions on encryption and anonymity, which are inherently unnecessary and disproportionate, and hence not legitimate as restrictions on freedom of expression, including as part of States' responses to terrorism and other forms of violence.
- Measures that weaken available digital security tools, such as backdoors and key escrows, since these disproportionately restrict freedom of expression and privacy and render communications networks more vulnerable to attack.

BOX 22. ECtHR* on Reasonable Suspicion

A former police officer was suspected of membership in a terrorist organization on the sole basis of his alleged use of an encrypted messaging service and placed in pre-trial detention.

The Court concluded that because the messaging service was not exclusively used by terrorists, his use of the service was insufficient to give rise to reasonable suspicion of membership of a terrorist organization, and therefore that his detention was unlawful.

Akgün v. Turkey * The European Court of Human Rights

161 <https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf>

162 Joint Declaration on Freedom of Expression and Countering Violent Extremism adopted by the UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Cooperation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, 03 May 2016.< https://www.osce.org/files/f/documents/e/9/237966.pdf>

11.2 Offensive Intrusive Technologies

Intrusive software allowing access to fixed and mobile devices so that the content of users' communications and other information including metadata (e.g. location, duration, source, and contacts) can be monitored covertly and remotely is commonly referred to as "spyware".

While in the past surveillance technology tended to be the exclusive concern of government agencies, in the modern era most of these technologies are developed by private firms which then sell to or otherwise put at the disposal of government agencies.[163]

Civil society groups employing computer forensic analysis have identified the widespread use of such technologies by repressive Member State agencies worldwide to target, inter alia, politicians, journalists, human rights defenders, and political dissidents. There is evidence that some of the targets are also subject to other human rights violations including extrajudicial killings and torture, or sexual and gender-based violence.[164]

States using such technologies are liable for all the associated human rights violations. However, States authorizing the trade or transfer of such technologies across international borders are at a minimum, are required to undertake some form of due diligence regarding the potential use of such technologies by the recipients and act accordingly, including by prohibiting transfers of intrusive technologies.[165]

The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression observed that:

> *"Analog surveillance tools, such as the wiretapping of a fixed line telephone or mobile phone, typically enables access to conversations – itself a potential problem but not the vast access to one's contacts, location data, keystrokes, video, and so on. It is containable in its aim both by judicial warrant and technology. Spyware like Pegasus, by contrast, may not be so limiting its intrusiveness is difficult to constrain. In legal terms, it may be difficult if not impossible for a state to demonstrate its use of spyware for narrow purposes and without "collaterally" sweeping in personal data having no relevance to a legitimate governmental purpose.*[166]"

163 For a partial list of such firms see: Position Paper of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, para. 17. Available at: https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

164 Position Paper of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, paras. 18-24.

165 See Human Rights Committee, General Comment 36, paras. 7 and 22-23.

166 D Kaye, 'The Spyware State and the Prospects for Accountability,' (2021) 27(4) Global Governance, p. 492.

Surveillance technology affects not only those persons whose data is actually collected, but also those whose data is never obtained because the threat of violations results in self-censorship. This chilling effect is all the more acute where spyware provides data not only about the targets but about all their contacts.[167] In a decision regarding the use of Pegasus spyware, the Supreme Court of India observed that "such a chilling effect on freedom of speech is an assault on the vital pubic watchdog role of the press, which may undermine the ability of the press to provide accurate and reliable information."[168]

As noted above, the use of arbitrary surveillance technologies can have a particularly dire impact on women as they are more likely to be subject to blackmail or discreditation as a result of actual or threatened exposure of real or fake sexualized content. Additionally, in private hands, sophisticated surveillance technologies raise the risk of intimate partner violence.[169]

The rate of spyware technological advancement is a source of alarm. For instance, while civil society has raised global concerns regarding the use of Pegasus, experts are able to detect the existence of Pegasus on targeted devices. This is not the case with a new technology developed by a company named Toka. This newer technology can not only divert live video feed but alter old feeds and erase any evidence of a covert operation, all without leaving any forensics or tell-tale signs of a hack. Company promotional materials assert that the technology can gather visual intelligence from both "live or recorded videos" and can "alter feeds" of "audio and visual" recordings to allow "masking of on-site activities" during "covert operations".[170]

The existence of such a technology raises critical rule of law concerns. For example, typically manipulated video is inadmissible as evidence in court. Therefore, Courts and parties to proceedings rely on the availability of technologies that can detect manipulation. Where manipulation is undetectable, the risk that a video will be altered to convict the innocent and acquit the guilty reaches dystopian proportions. Moreover, technologies that cannot be detected may make remedies for misuse virtually impossible. Consequently, the use of a technology such as the one developed by Toka can not be consistent with international human rights law, or at least until such a time as a technology is developed that can detect its use.

With respect to other forms of spyware, Member States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises by establishing legal frameworks regulating the use of high-risk commercial products, such as spyware, by domestic security forces, ensuring that spyware is not used in a discriminatory manner, that there is effective and independent ongoing and post facto oversight, and that where the unlawful use of spyware is detected, victims have access to an effective remedy.

States are required to adopt adequate legislative ad operational measures to protect persons within their jurisdiction from unlawful interference with their human rights by private sector actors,[171] as also set out in the Guiding Principles on Business and Human Rights.

The topic of international regulation of the commercial spyware technology industry and trade is likely to be a key focus of discussions at the international level in coming years.[172]

167 A/HRC/51/17, para. 12.

168 See summary of Supreme Court of India, Manohar Lal Sharma v Union of India, Order of 27 October 2021, including para. 39, at https://globalfreedomofexpression.columbia.edu/cases/manohar-v-union-of-india/

169 Position Paper of the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach, paras. 52, 55.

170 https://www.haaretz.com/israel-news/security-aviation/2022-12-26/ty-article-magazine/.premium/this-dystopian-cyber-firm-could-have-saved-mossad-assassins-from-exposure/00000185-0bc6-d26d-a1b7-dbd739100000

171 See Human Rights Committee, General Comment 36, paras. 7 and 22-23.

172 Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 'Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach' (April 2023); European Parliament, Committee of Inquiry to investigate the use of Pegasus and equivalent surveillant spyware, 'Draft Report' (28 November 2022).

[XII]

Internet Shutdowns

12.1 Internet Shutdowns

Internet shutdowns are measures taken by a government, or on behalf of a government, to intentionally disrupt access to, and the use of, information and communications systems online. They include actions that limit the ability of a large number of people to use online communications tools, either by restricting internet connectivity wholesale or by obstructing the accessibility and usability of the internet, social media and communication services, by 'throttling' bandwidth. In some cases, shutdowns of entire telephone networks accompany internet shutdowns, leaving no channel for direct electronic communication. Between 2016 and 2021, internet shutdowns were documented in 74 countries, with some countries blocking access repeatedly and over long periods of time.[173]

The results of such shutdowns are often dire. Shutdowns have been used to interfere with the right to peaceful assembly, often in the context of protests and political crisis, to damage democratic electoral processes and the free flow of information. Internet shutdowns have serious repercussions on all economic sectors and impact on access to essential services that increasingly rely on digital tools and communications, such as education, health care, social assistance and humanitarian assistance.[174] Shutdowns may have a particularly grievous impact on women and girls, undermining their access to critical support and protection, including emergency health support, information related to reproductive health issues, and exacerbating the gender divide.[175] They can also interfere with career and educational opportunities.[176]

Internet shutdowns have a detrimental impact on many human rights, and most immediately on the right to freedom of expression and access to information. Internet shutdowns generally do not meet the requirements of having an adequate basis in domestic law/ legal certainty, legitimate aim, necessity and proportionality as defined under international human rights law.[177]

When implementing shutdowns, governments often fail to acknowledge them or provide minimal or no explanation for the measures, including their legal basis and underlying grounds. When shutdowns are based on legal orders, they generally rely on vaguely formulated laws that offer a large scope of discretion to authorities. Official justifications

173 Report of the Office of the United Nations High Commissioner on Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, paras. 5-6, and 19. <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>

174 *bid.*, paras. 25-26, 33, 35-37.

175 *Ibid.*, para. 38.

176 See, Access Now: <https://www.accessnow.org/internet-shutdowns-international-womens-day/>

177 Report of the Office of the United Nations High Commissioner on Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, paras. 9,13

of a large majority of shutdowns have often focused on public safety and national security or the need to restrict the circulation of information deemed illegal or likely ot cause harm. According to data compiled by civil society groups, 189 shutdowns between 2016 and 2021 were justified by public safety concerns, while 150 were based on national security grounds. Many of those shutdowns were followed by spikes in violence, which suggests that such interventions often fail to achieve their officially stated safety and security objectives.[178]

BOX 23. Member State J Shuts Down Internet and Communication Services for Two Years

On counter-terrorism grounds, Member State J shut down the internet and communications services to region Y, home to a population of 6 million persons, for two years from 2020–2022. Among the numerous devastating impacts on the civilian population in this predominantly agricultural region, subsistence farmers were unable to obtain or share meteorological information, and the population more generally was unable to receive remittances from abroad on which it depends upon.

BOX 24. Blocking Wikipedia in Member State L

Member State L has blocked Wikipedia for over a year. In announcing the restriction of Wikipedia, State authorities cited the government's authority to block access to web pages or entire websites as deemed necessary.

Internet shutdowns very rarely meet the proportionality test, given their indiscriminate and widespread impacts. Their adverse effect on a wide range of human rights often extends beyond the areas or periods of their implementation, rendering them disproportionate, even when they are meant to respond to genuine threats.[179]

The Human Rights Committee has indicated that generic bans on the operation of certain sites and systems are also incompatible with the right to freedom of expression.[180] The United Nations High Commissioner for Human Rights has recommended that States refrain from the full range of Internet shutdowns, blanket shutdowns in particular. Targeted shutdowns of a communications service provided through the Internet may be deemed proportionate and justifiable only in the most exceptional circumstances, as a last resort when necessary to achieve a legitimate aim, such as national security or public order, and when no other means are effective to prevent or mitigate those harms. Should States nevertheless consider implementing shutdowns, the High Commissioner for Human Rights recommended strict adherence to six essential requirements, including the meeting requirements of having an adequate basis in domestic law/ legal certainty, legitimate aim, proportionality as well as providing prior authorization by a court or another independent adjudicatory body, communicating in advance to the public and telecommunications or Internet service providers, with a clear explanation of the legal basis and details on the Internet shutdown's scope and duration, as well as ensuring access to meaningful redress mechanisms to those whose rights have been affected by the shutdowns, including through judicial proceedings that present due process guarantees.[181]

178 Report of the Office of the United Nations High Commissioner on Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, para. 31. <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>

179 *Ibid.*, paras. 13 and 59..

180 Human Rights Committee, General Comment No. 34 (Article 19: Freedoms of opinion and expression), CCPR/C/GC/34, 12 September 2011, para. 43.

181 Report of the Office of the United Nations High Commissioner on Human Rights, Internet shutdowns: trends, causes, legal implications and impacts on a range of human rights, A/HRC/50/55, paras. 13, 66-67, <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>

BOX 25. Surveillance Law in Member State K

The surveillance laws passed in Member State K after a major terrorist attack allowed national authorities to monitor and block websites with no judicial oversight.

[XIII] Conclusion

13.1 Overview

Counter-Terrorism programmes and measures must be Human Rights compliant to ensure consistency with international law and prevent the creation or exacerbation of grievances that can result in violence. Consequently, Member States and their agencies must adopt legislation and practices consistent with the following:

13.2 Summary Recommendations

TABLE 2. **Summary Recommendations**

Definitions of Terrorism and Incitement to Terrorism	Definitions of terrorism and incitement to terrorism consistent with those established by the Security Council and Special Rapporteur on counter-terrorism and human rights.
Surveillance and Online Data Collection	Surveillance and online data collection interfere with privacy rights. Therefore, the following must be taken into account: • Any such interference must be a) provided by law, b) pursue a legitimate aim, and c) necessary and proportionate. • Any such interference must be authorized by an independent body on a case-by-case basis, and carefully circumscribed to ensure that the data sought, and the retention of the data, are not overly broad. • Surveillance programmes must be subject to independent oversight. • Victims of unlawful surveillance must have a right to an effective remedy. • Member States must recognize that the collection and use of metadata can be as intrusive as the collection and use of the content of communications.

Prohibition of Discrimination	• Surveillance, or the collection of data, on discriminatory grounds is never permissible. • The use of biometrics tools including facial recognition on discriminatory grounds is never permissible. • Victims of discrimination are entitled to a remedy.
Internet and Social Media	• Open-source investigations must serve a legitimate aim, be proportionate to that aim and non-discriminatory. • In the context of counter-terrorism measures, Member States, and Member State authorities, must not seek data regarding individuals or groups not engaged in violence or the threat of violence as set out in human rights compliant definitions of terrorism and incitement to terrorism. • In the context of counter-terrorism measures, Member States, and their agencies, must not seek the removal of content by ICT companies that do not fall within the human rights compliant definitions of terrorism and incitement to terrorism or other content protected under human rights law. Legal including criminal justice in connection with incitement to terrorism must respect the principle of legality/ legal certainty, relevant due process and fair trial rights, be proportionate and not unduly restrict human rights including freedom of expression.
Special Investigative Techniques	• Member States must clearly set out in their national legislation the circumstances in which and the conditions under which the competent authorities are empowered to resort to the use of Special Investigative techniques with due consideration for the human rights implications linked to their intrusive nature. For this reason, special Investigative techniques should only be used to address serious crimes and should be accompanied by adequate safeguards against abuse including meaningful independent monitoring and oversight.
Circumvention Technologies	• Circumvention technologies are predominantly used for lawful purposes and therefore must not be banned.
Internet Shutdowns	• Internet shutdowns have a detrimental impact on a series of human rights, and most immediately on the right to freedom of expression and access to information. Internet shutdowns generally do not meet the requirements of legal certainty, legitimate aim, necessity and proportionality as defined under international human rights law.

United Nations Office of Counter-Terrorism
United Nations Headquarters
New York, NY 10017

www.un.org/counterterrorism

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)