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

INTERPOL

Funded by
the European Union

Cybersecurity and **New Technologies**

Establishing Legislative Framework, Transparency Mechanisms and Oversight for Online Data Collection

---

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.

United Nations Office of Counter-Terrorism

United Nations Headquarters

New York, NY 10017

www.un.org/counterterrorism

200, Quai Charles de Gaulle
69006 Lyon, France

www.interpol.int/en

Contents

Joint Foreword

Advances in Information and Communication Technologies 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 Coordination 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 review by a wide range of stakeholders. Specifically, the United Nations Office of Counter-Terrorism (UNOCT) wish to acknowledge the contribution made by:

- **Mr. Kamel El Hilali – PhD in Law**
  Paris Pantheon Assas University

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 analysing.
Criminal Justice Process	A legal process to bring about criminal charges against an individual or an entity and the court proceedings judgement of the case, sentencing of the conviction 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]
Effective Oversight Mechanisms	are independent, equipped with appropriate and adequate expertise, competencies and resources, have full and unhindered access to information, premises and officials and have mandates and powers defined in law to scrutinize compliance with applicable law, including human rights, initiate investigations and adequately investigate official misconduct.
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[2]
Impartial Oversight Mechanisms	are those that make decisions on the basis of facts and in accordance with the law, without any restrictions, improper influences, inducements, pressures, threats or interferences, direct or indirect, from any quarter or for any reason.[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 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

3 Office of the United Nations High Commissioner for Human Rights, Basic Principles on the Independent of the Judiciary, < https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-independence-judiciary>

Independent Oversight Mechanisms	are autonomous from political, economic, military or other objectives. They have: 1) formal (de jure) independence requiring that they remain outside the bureaucratic, hierarchical chain of command within a ministry or other government agencies; and 2) actual (de facto) independence, which relates to the agency's self-determination in the use of appropriate measures.[4]
Intelligence	The product resulting from collecting, developing, disseminating, analysing, 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.
Legal Framework for Government Access to Personal Data	refers to national laws, executive or judicial orders, administrative regulations, case law, and other legally binding instruments or requirements, including legal obligations arising from international and supranational law as applicable in the country.
Metadata	defined as "a set of data that describes and gives information about other data."
New Technologies	While the new technologies terminology covers a wide range of different technologies[5], 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.[6]
Personal Online Data	Refers to any online information relating to an identified or identifiable individual
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.
Surveillance	the systematic observation or monitoring of individuals, groups or activities by an authorized government entity, including the collection, recording, analysis, or dissemination of information, for the purpose of preventing, investigating, and/or prosecuting criminal activity. It may consist of physical, electronic (wiretaps, tracking devices, etc.) or digital surveillance (internet browsing, email communications, social media interactions).
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.[7]
Zettabyte	One zettabyte is equal to one billon terabytes.

4 See, for example, OECD Public Integrity Handbook Section 12.2.3, <https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en>

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

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

7 United Nations Security Council resolution 1566 (2004), OP 3.

Executive Summary

The most effective counter-terrorism responses are those that are compliant with international human rights obligations. Intrusive national security policies may have a negative impact on the respect and protection of human rights, in particular the rights to privacy, freedom of expression and association, and non-discrimination. Whether online or offline, ensuring that security policies comply with international law obligations requires the adoption of appropriate and human rights-compliant legal frameworks and the establishment of effective and independent transparency and oversight mechanisms.

This guidance focuses on the obligations of Member States and not those of Information and Communications Technology companies. The human rights responsibilities of these companies are addressed in the United Nations Guiding Principles on Business and Human Rights.[8]

8 Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework | OHCHR

[1]

Background

1.1 Overview

United Nations Member States attach great importance to addressing impact of new technologies in countering terrorism. During the seventh review of the of the United Nations Global Counter-Terrorism Strategy (A/RES/75/291)[9] 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)[10] and 2396 (2017)[11] 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[12], 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 the 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 terrorist purposes was discussed at the dedicated special meeting of the United Nations Security Council Counter-Terrorism Committee's (CTC), which took place on 28-29 October 2022 in New Delhi and resulted in the adoption of a non-binding document, known as the Delhi Declaration[13].

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

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

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

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

13 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

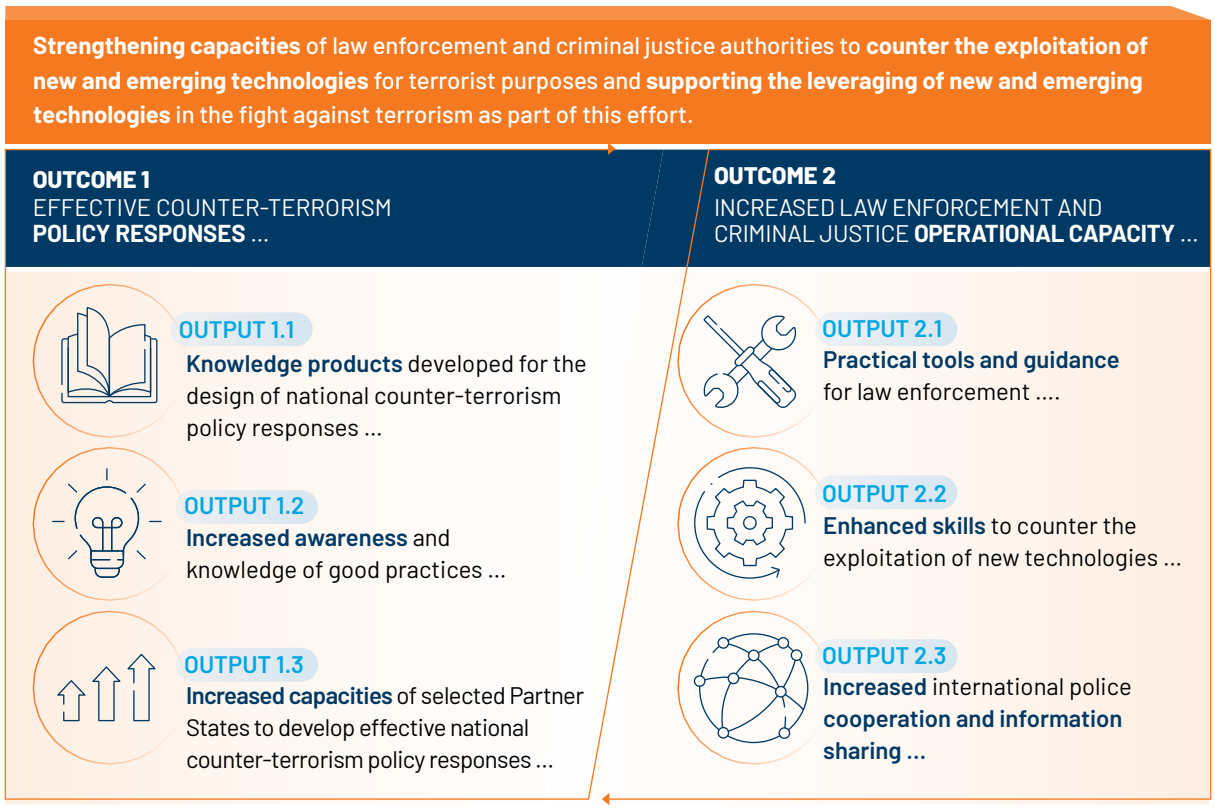


TABLE 1. **CT TECH Outcomes and Outputs**

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 is 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 rule of law.	
Output 2.1	Practical tools and guidance for law enforcement on countering 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 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 the 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 provide guidance on the establishment of independent and effective transparency and oversight mechanisms for online surveillance and online data collection related to counter-terrorism.

1.3.1 Scope

This document aims to raise awareness regarding the human rights and privacy concerns on the practices of online data collection for counter-terrorism law enforcement purposes as well as offer key oversight considerations to ensure appropriate safeguards to the practices of online data collection with respect to international human rights norms and practices.

1.3.2 Target Audience

This guide is designed primarily for policy makers, although law enforcement agencies should be aware of its main principles and related mechanisms.

1.3.3 Benefits

History is replete with examples of responses to terrorist threats that have created or amplified existing grievances that may in turn fuel terrorism and violent extremism conducive to terrorism. Effective independent oversight mechanisms contribute to greater accountability and transparency.

1.3.4 Limitations

This guidance does not address in any depth the numerous concerns regarding the purchase of commercially aggregated personal data by government agencies, although the practice raises substantial privacy issues. It also does not address oversight of the private sector.

[II]

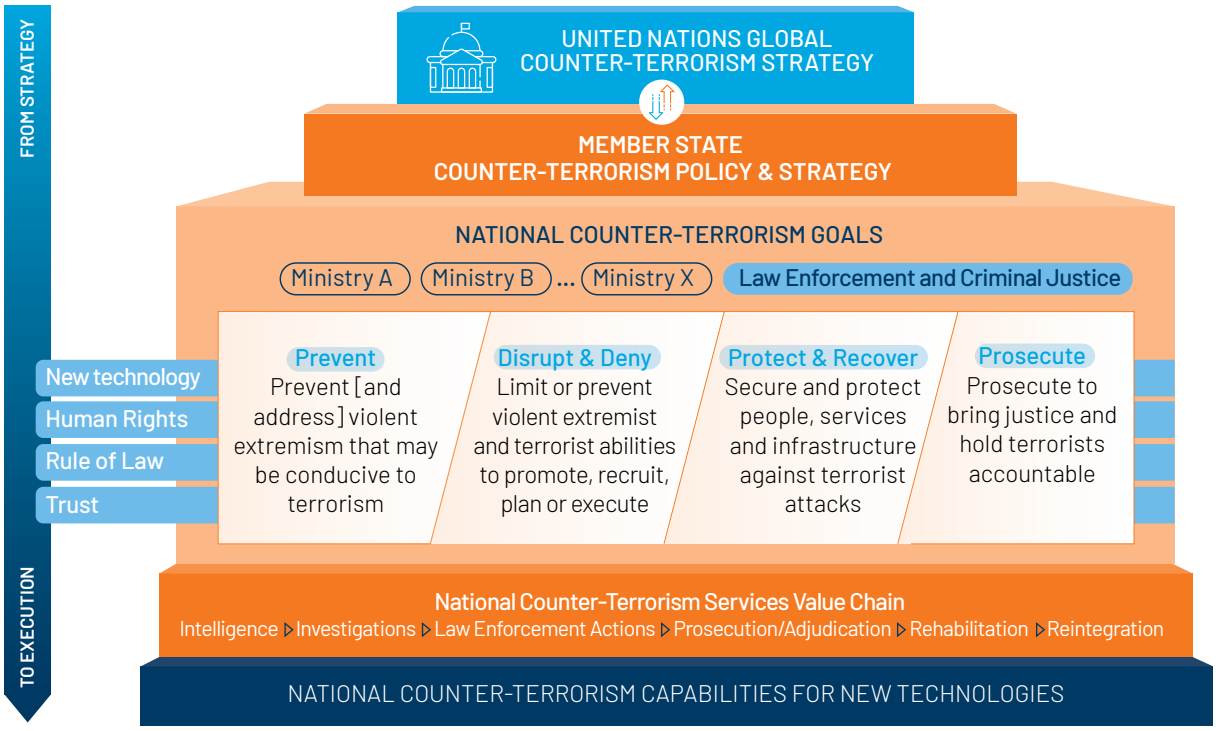
Approach

2.1 Overview

The report seeks to support and enable Member States to enhance compliance with international human rights norms and standards in leveraging new technologies to prevent and counter-terrorism, with a focus on the establishment of effective and independent transparency and oversight mechanisms for online surveillance and online data collection related to counter-terrorism. It seeks to support the development of effective counter-terrorism policy responses which are aligned to the United Nations Global Counter-Terrorism Strategy and in full respect of the rule of law and international human rights norms and standards.

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 as and when 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**

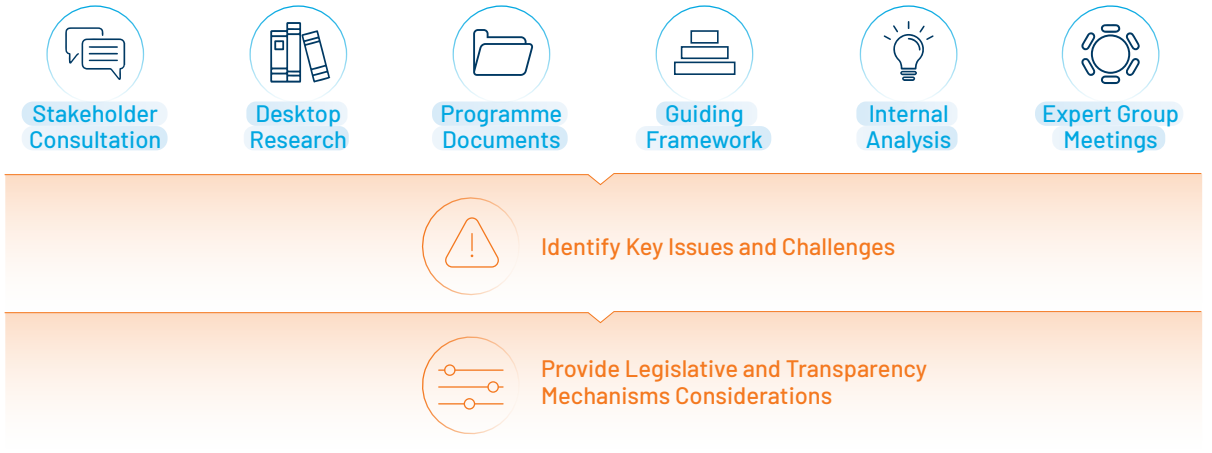
Services	Description
Criminal Justice Process	A legal process to bring about criminal charges against an individual or an entity and the court proceedings, judgement of the case, and sentencing of the conviction as well as corrections and rehabilitation.
Intelligence	The product resulting from collecting, developing, disseminating, analysing, 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



The methodology for developing this document on "Establishing Legislative Frameworks and Transparency Mechanisms for Online Data Collection" includes research, analysis, and consultation with relevant stakeholders and experts, which include CT TECH project documents, stakeholder consultation, internal analysis, desktop research, expert group meetings, co-ordination with the United Nations Global Counter-Terrorism Coordination Compact entities, and the guiding framework as described above in section 2.2. From these activities, the key outputs of this document identify key human rights and privacy issues and challenges with regard to online data collection as well as offer key considerations for oversight through legislative and transparency mechanisms.

2.3.1 Expert Group Meetings and Consultation

This guide has been developed with input from experts through Expert Group Meeting (EGM) sessions as well as individual consultations and reviews. The EGM brought together a group of experts and practitioners from counter-terrorism and law enforcement agencies, human rights experts, private sector, academia and civil society to discuss how to counter the 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, with respect for human rights and the rule of law as the fundamental basis, in line with international law, including international human rights law, international humanitarian law, and international refugee law.

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	United Nations Global Counter-Terrorism Strategy.
2	Reports of the Office of the United Nations High Commissioner for Human Rights, the Right to Privacy in the Digital Age.
3	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.
4	The state of international cooperation for lawful access to digital evidence: research perspectives, CTED trends report, January 2022.
5	The Tshwane Principles on National Security and the Right to Information
6	UNODC, Handbook on police accountability, oversight and integrity.
7	OECD Public Integrity Handbook
8	Council of Europe, Practical guide on the use of personal data in the police sector
9	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

[III]

Introduction

3.1 Overview

As advancements in technology continue to accelerate, terrorists increasingly misuse these innovations to further their destructive agendas. The terrorist exploitation of the rapid proliferation of communication platforms, social media networks, encryption techniques, and emerging technologies pose significant challenges for law enforcement authorities. The integration of technology into the arsenal of terrorist groups poses unprecedented challenges, requiring governments to reassess their strategies and adapt their approaches.

In formulating counter-terrorism policies, Member States must recognize the critical need to understand, anticipate, and effectively respond to terrorists' exploitation of emerging technologies. Such policies focus on a range of aspects, including awareness, threat interventions, national counter-terrorism capabilities, cooperation, and capacity-building initiatives. By adopting comprehensive, agile and human rights-compliant national counter-terrorism policies, governments aim to stay ahead of the curve, proactively mitigating the risks associated with terrorists' misuse of new technologies while safeguarding the security and rights of persons within their jurisdiction, including the right to privacy.

3.2 New Technologies and Counter-Terrorism

Today, the advancements of digital technologies, data, and the Internet have led to a hyperconnected world in which information is accessed, shared, and received nearly instantaneously. As of 2022, nearly 70% of the global population uses the Internet[14], of which over 93 percent are social media users[15]. Globally, it is estimated that in 2022 over 97 zettabytes[16] of information was generated.[17] Whilst such technology advancements provide the opportunity to transform society for the greater good, terrorist actors are taking advantage of the same technology for their own violent purposes. The use of new technologies for terrorist purposes poses significant challenges to Member States in countering terrorism – in particular – the use of technologies that allow for anonymity and the ability to coordinate and operate remotely.

14 ITU Global Connectivity Report 2022, https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/index/

15 Domo Data Never Sleeps, Data Never Sleeps 10.0 | Domo

16 1 zettabyte equals to 1 billion terabytes

17 Statista, Total data volume worldwide 2010-2025 | Statista

On the other hand, new technologies present significant opportunities as a capability multiplier for counter-terrorism and law enforcement authorities. For example, such technologies could allow law enforcement authorities to do more with less, fast track timely decision making, generate new insights, and conduct disruptive operations remotely. At the same time, concerns arise about the risks to privacy and the exercise of human rights more generally, emanating from relevant legislation allowing the use of such technologies which often fall short of applicable international human rights standards as well as from their implementation by law enforcement.

Countering the use of new technologies for terrorist purposes hinges on understanding how terrorist actors are using new technologies, developing effective and human rights-compliant legal framework and policy responses, and building operational capacity to counter the use of such technologies for terrorist purposes, to include leveraging and adopting the use of new technologies.

3.2.1 Challenges – Use of New Technologies for Terrorist Purposes

Advances in Information and Communication Technologies (ICT) and their availability have made it attractive for terrorist and violent extremist groups to exploit the Internet and social media to facilitate a wide range of activities, including incitement to terrorism, radicalization to violence, recruitment, training, planning, collection of information, communication, preparation, terrorist propaganda, and financing. Terrorists also use encrypted communications and the dark web to share terrorist content, expertise, such as designs of improvised explosive devices and attack strategies, as well as to coordinate and facilitate attacks and procure weapons and counterfeit documents. Meanwhile, developments in the fields of artificial intelligence, machine learning, 5G telecommunications, robotics, big data, algorithmic filters, biotechnology, self-driving cars, and drones may suggest that once these technologies become commercially available, affordable, and convenient to use, they could also be misused by terrorists to expand the range and lethality of their attacks.

3.2.2 Opportunities – Counter-Terrorism Law Enforcement

New technologies present valuable opportunities for law enforcement agencies to effectively counter-terrorism when harnessed in compliance with international human rights law. Law enforcement can make use of new technologies to detect, investigate, prosecute, and adjudicate terrorist-related offences in new and more effective ways.

Open-source intelligence enables quick collection of information about targets of interest, which can make law enforcement activities more effective. Advanced data analytics and artificial intelligence (AI) capabilities allow for the processing and analysis of vast amounts of information, enabling law enforcement to identify patterns, detect potential threats, and preemptively respond to terrorist activities. Advanced surveillance systems, including facial recognition and biometric technologies, aid in the identification and tracking of suspects, enhancing the efficiency of investigations, preventing potential attacks, and prosecuting suspected terrorists. Furthermore, digital forensics tools assist in extracting critical evidence from electronic devices, enabling law enforcement to uncover hidden connections, disrupt terrorist networks and prosecute suspected terrorists.

Leveraging new technologies can help prioritize limited law enforcement resources in a more effective way. However, it is crucial that these technologies are employed ethically and with strict adherence to the rule of law and international human rights norms and standards, including the right to privacy. Transparency and accountability measures and mechanisms must be in place to ensure responsible use and prevent any potential misuse of these powerful tools. Additionally, comprehensive training programmes should be implemented to equip law enforcement personnel with the necessary skills to leverage new technologies effectively in line with international human rights norms and standards, and within the boundaries of legal and ethical frameworks. By leveraging new technology responsibly, law enforcement can significantly enhance their counter-terrorism efforts and safeguard the safety and security of communities.

3.2.3 Human Rights and New Technologies

Terrorism poses a serious challenge to the very tenets of the rule of law, the protection of human rights and their effective implementation. It can destabilize legitimately constituted governments, undermine pluralistic civil society, jeopardize peace and security, and threaten social and economic development. States have the obligation to take appropriate measures to protect persons within their jurisdiction against reasonably foreseeable threats of terrorist attacks. States' duty to safeguard human rights includes the obligation to take necessary and adequate measures to prevent, combat and punish activities that endanger these rights, such as threats to national security or violent crime, including terrorism. All such measures, must themselves be in line with international human rights law and rule of law standards.

In the context of employing new and emerging technologies to counter terrorist activities , States have to ensure that relevant laws, policies and practices respect rights such as the right to privacy, the rights to freedom of expression, freedom of association, freedom of thought, conscience and religion, the right to liberty and security of the person, the right to fair trial, including the presumption of innocence as well as the principle of non-discrimination. States must also uphold the absolute prohibition of torture and cruel, inhuman or degrading treatment or punishment.

The UN, Interpol and the EU have repeatedly underlined the interrelationship between new technologies, counter-terrorism, and human rights, including gender equality. The UN Global Counter-Terrorism Strategy and various General Assembly and Security Council resolutions underscore Member States' obligations under international human rights law, international humanitarian law, and international refugee law when countering terrorism .In particular, the UN's counter-terrorism strategy recognizes that "effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing" and requires measures to ensure respect for human rights for all and the rule of law as the fundamental basis of the fight against terrorism . Specifically, the Strategy encouraged Member States to address 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 while respecting international law, including international human rights law, including the right to freedom of expression.

3.2.4 Gender, Technology and Policy Response

Gender refers to the roles, behaviors, activities, and attributes that a given society at a given time considers appropriate for men and women, girls and boys. In addition to the social attributes and opportunities associated with being male and female, gender is also relevant for the relationships between women and men and girls and boys. Gender is part of the broader socio-cultural context, and intersects with other identity factors, including sex, class, race, poverty level, ethnicity, sexual orientation, age, among others. Men, women, girls and boys, as well as persons of different gender identities and expressions experience security differently and in accordance to their particular needs, vulnerabilities and capacities.[18] Specifically in the use of new technologies, while the absence of hierarchical structures on the internet may remove gender constraints, and provides opportunities for empowering women, it also bears an increased likelihood for them to be recruited or actively engaged with violent extremist and terrorist groups online.[19] Evidence suggests that, for their purposes, terrorist groups expertly exploit and manipulate gender inequalities, norms, and roles, including concepts of masculinities. For example, Da'esh skillfully recruited women through social media, adapting their messages to appeal to women speaking different languages and living in different social, economic and cultural contexts in Western Europe, Central Asia, and Middle East and North Africa, often tapping into women´s experience of gender inequalities . Another critical aspect regarding gender and new technologies refers to the digital gender divide, whereby globally, women´s access to the internet is estimated to be at 85 per cent that of men with approximately 1.7 billion women in the Global South lacking access. This disparity poses a human rights concern underlying all dimensions of cybersecurity, including the potential exposure, insecurity, or participation in governance.[20]

18 DCAF, OSCE/ODIHR, and UN Women, Gender and Security Sector Reform Toolkit (Geneva: DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit

19 CTED, 'Gender Dimensions of The Response to Returning Foreign Terrorist Fighters - Research Perspectives', February 2019.

20 DCAF, 'Gender Equality, Cybersecurity, and Security Sector Governance – Understanding the role of gender in cybersecurity governance'. January 2023

[IV] Collection of Online Data by Law Enforcement Authorities

4.1 Overview

As technological advances accelerate, terrorists increasingly exploit communication platforms, social media networks, encryption techniques, and other new and emerging technologies to recruit and organize members, acquire weapons, finance operations, and otherwise plan, support, commit, and cover up acts of terrorism. At the same time, these same technologies provide law enforcement with new tools to identify potential terrorist suspects, monitor the membership of terrorist entities, surveil their activities, and disrupt their operations. However, as new technologies facilitate identification, surveillance, and control, threats to fundamental rights, including the rights to privacy, freedom of expression and association, and the right to non-discrimination, have soared, and national security grounds are often misused to justify intrusive online data collection. While relevant technologies may be new, the dangers associated with unregulated surveillance are not. As early as 1978, the European Court of Human Rights observed 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".[21] Similarly, the United Nations Global Counter-Terrorism Strategy recognizes "that effective counter-terrorism measures and the protection of human rights are not conflicting goals, but complementary and mutually reinforcing".[22] Nonetheless, Member States have routinely engaged in the electronic and digital surveillance of civil society actors, journalists and people who simply disagree with their governments and used the information collected to target, repress and silence under the guise of national security.

In response to growing concerns about the rapid acceleration of government surveillance facilitated by new technologies, the General Assembly adopted Resolution 73/179, affirming the Right to Privacy and calling upon states 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."[23] Effective oversight and appropriate redress, including through judicial review and other legal means are principles reiterated in the seventh and eighth reviews of the United Nations Global Counter-Terrorism Strategy.[24]

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

22 A/RES/60/288, Preambular para. to pillar IV.

23 A/RES/73/179, O.P 6 (d).

24 A/RES/75/291, para. 106 (seventh review), A/RES/77/298, para. 110 (eighth review).

Best practices and mechanisms must include: clear and precise internal guidelines for law enforcement access to online data to be provided to the relevant officers before they access any personal data; internal supervision of data collection during operations; ex ante independent authorization for the collection of certain types of information; independent oversight of law enforcement operations during and after operations; and, access to redress mechanisms and the provision of effective remedies and to victims of violations of human rights.

4.2 Terminology: Online Data Collection and Online Surveillance

Although often used interchangeably, there are differences between the terms "online data collection" and "online (or digital) surveillance." Online data collection refers to the process of gathering, storing, and processing of information about individuals and their online activities. Information can be collected by website cookies, user registration, online surveys, etc. In Europe, in particular, such collection requires the user's knowledge and consent. With respect to all government activities, online personal data collection must be regulated, serve a legitimate purpose set out in law, be proportionate and necessary to achieve this legitimate purpose and be used for this purpose[25] but collection and processing of that data does not necessarily require prior independent authorization and strict oversight.

A police officer who has stopped a vehicle for a traffic infraction, for example, may not need prior judicial authorization to check the driver's license against a database of drivers whose licenses have been suspended or the license plate against a database of stolen vehicles. Moreover, licensed drivers are aware that their personal data is collected, stored, and processed by government agencies for road safety purposes.

That being said, access to certain categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance, additional security measures, and of an organisational nature. Safeguards should be adjusted to each data processing operation taking into account their specificities. The use of multiple levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.) is highly recommended. Further, it is of paramount importance that specific security measures be put in place to prevent unauthorised or unwanted access to those categories of data.[26]

In contrast to ordinary data collection and processing, online surveillance, involves the monitoring of the online activities of specific individuals and entities by security forces, typically without their knowledge or consent. The absence of knowledge and consent calls for more stringent oversight if not complete transparency at all times.

As all forms of surveillance - physical, electronic, and digital - generally raise more critical privacy issues, they require more rigorous oversight than other forms of personal data collection. This guidance focuses primarily on personal data collection in the context of surveillance operations.

25 See for example, Council of Europe, Practical guide on the use of personal data in the police sector, Sections 2 and 3. Available at: < https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>

26 Council of Europe, Practical guide on the use of personal data in the police sector, Section 4. Available at: < https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>

4.3 Metadata

Metadata 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. The European Court of Human Rights, for example, held that communications data is an "integral element" of a private communication and therefore enjoys a degree of protection under Article 8 albeit less than that afforded to the content of a communication.[27] 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 call 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 the protected content of communications, and as a result, collection of such data can be highly intrusive.[28] Indeed, a separate European court, the Court of Justice of the European Union, 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. In particular, that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".[29] Consequently, distinctions between identifying personal data and apparently anonymized metadata are increasingly artificial and difficult to justify.

4.4 Guiding Principles

Under international human rights law, it is possible for States to derogate from[30] and impose limitations on the exercise of certain rights. Some rights are however absolute and cannot be derogated from or restricted.[31] For the purpose of this guidance, the below will focus on the conditions for limitations of qualified rights. Any interference with a qualified human right, such as the rights to privacy and freedom of expression and association 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 measure must also be governed by the principles of necessity and proportionality. As such, restrictions on human rights must always respect the prohibition of discrimination.[32]

27 See, European Court of Human Rights, *Big Brother Watch and other v. the United Kingdom and Malone v. United Kingdom*, (1985), para. 84.

28 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>

29 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. 117.

30 When facing a public emergency "threatening the life of the nation", States have the possibility to temporarily adjust certain human rights obligations, subject to a set of conditions. For more details on derogations: Human Rights Committee, General Comment No. 29 'States of emergency (Article 4), CCPR/C/21/Rev.1/Add.11.

31 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.

32 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.

4.4.1 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 such as independent review and oversight and must for provide for an effective remedy, in case of violations of human rights. Foreseeability implies that the law must be formulated with sufficient precision to enable both an individual to regulate their conduct accordingly[33] and competent authorities to ascertain when rights can be restricted and indicate the scope of any discretion conferred them as well as the manner of its exercise.[34] The law must be sufficiently accessible so that individuals must have the possibility to become aware of its content.[35] A decision to authorize interference with the right to privacy, 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.[36] Secret rules, guidelines, or interpretations of the rules do not have the quality of "law."[37] Finally, laws must be democratically enacted.[38]

4.4.2 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."[39] "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".[40]

However, States have at times improperly referred to the imperatives of national security, specifically counter-terrorism, as a pretext to justify vaguely defined and arbitrary interferences with human rights. "[t]he 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.[41]

33 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.

34 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.

35 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.

36 Human Rights Committee, General Comment 16, para. 8, available at: https://www.refworld.org/docid/453883f922.html

37 Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, A/HRC/27/37, para.29. See also, European Court of Human Rights, *Malone v. United Kingdom*, (1985), 7 EHRR 14, paras. 67-68, available at: https://www.stradalex.com/nl/sl_src_publ_jur_int/document/echr_8691-79; African Commission on Human and Peoples' Rights, Principles and Guidelines on Human and Peoples' Rights While Countering Terrorism in Africa, Part 11, A: The legal framework concerning any interference with privacy, as well as their procedures, should be accessible to the public. Available at: https://www.achpr.org/legalinstruments/detail?id=9

38 See, African Court of Human and Peoples' Rights, *XYZ v. Republic of Benin*, Judgement 27 November 2022, paras. 101-102, concluding that the impugned law was unlawfully adopted by summary procedure, and that the additional failure to disseminate the law constituted a violation of the right to information, paras. 118-121. Available at: https://africanlii.org/afu/judgment/african-court/2020/3

39 See for example, ECHR, Article 8 (2); IACHR, Articles 13 (2)(b) and 30; ACHPR, Article 11. See also, African Commission on Human and Peoples' Rights, Principles and Guidelines on Human and Peoples' Rights While Countering Terrorism in Africa, General Principle M.

40 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.

41 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>

4.4.3 Necessity and Proportionality

As such, limitations must not only be taken in pursuance of a legitimate aim, they must also be necessary to protect the aim. The requirement of necessity goes beyond/ 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.

Measures restricting a qualified right must be proportionate to the legitimate aim pursued, and , they must be appropriate to achieve their protective function and they must be the least intrusive among those that might achieve the desired result, and they must be proportionate to the interest to be protected.[42] For example, in a case before the European Court of Human Rights, the Court 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 Court 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.[43]

4.4.4 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.[44] Protected grounds comprise, but are not limited to: sex, race, colour, ethnic origin, language, religion, political or other opinions, national or social origin, or other status.

4.5 Rights of Data Subjects

There is little international law on the rights of data subjects. Relevant European Union Law prohibits arbitrary interference with, inter alia, rights to privacy, freedom of expression, including the right to seek information, [45] the right to freedom of association and the prohibition against discrimination.

42 See for example, Human Rights Committee, General Comment 31, para. 6. 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>

43 European Court on 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.

44 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.

45 Freedom of Information is an integral part of the fundamental right to freedom of expression. See, for example, < https://www.un.org/ruleoflaw/thematic-areas/governance/freedom-of-information/#:~:text=Freedom%20of%20information%20is%20an,right%20of%20freedom%20of%20expression>

At its essence, European Union law requires that, at a minimum, the persons affected by online data collection and processing have a right to know that personal data has been retained and processed, to have access to the data stored, to rectify data that is inaccurate or outdated, and to delete or rectify data unlawfully or unnecessarily stored. In addition, they have a right to object to personal data processing, unless the State or processing entity demonstrates legitimate grounds for the collection and processing of that data and they have the right to a remedy where their rights have been violated.[46]

However, there may be restrictions from these general rules in the context of law enforcement activities and operations when such restrictions are provided by law, respect the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society, including for, but not limited to the protection of national security or the prevention, investigation and prosecution of criminal offences.[47] For example: when investigating and surveilling a high-risk suspect, data processing and long-term data retention may be justified without informing the individual under surveillance if alerting the target could prejudice an ongoing or planned investigation. But once the purpose of covert monitoring has been achieved, and no other restriction is applicable, the target should be informed about the fact that s/he was subject to such a measure. Other circumstances in which restrictions on the right to access information related to data processed might be warranted include, for example, if providing information to a data subject could endanger the safety of a witness or informant. Or, if specific intelligence indicates that money laundering operations have been carried out to finance terrorist operations, data collected on individuals may be kept, if approved by an external oversight body, for a longer period than might otherwise be strictly necessary for purposes of an individual investigation. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified. [48]

46 Council of Europe, modernized Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. See also article 21 of the European Union's General Data Protection Regulation and article 18 (1) of the Malabo Convention on cyber security and personal data protection.

47 *Ibid.*, Article 11.

48 Council of Europe, Practical guide on the use of personal data in the police sector, Sections 5,7. Available at: < https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5>

[V] Transparency and Oversight Mechanisms

5.1 Overview

Although there are very few, if any, international or regional instruments that specify the type of oversight mechanisms required of Member States, procedural obligations flow from substantive obligations. The European Court of Human Rights has held that in order to secure rights and freedoms, the Convention does not just oblige the higher authorities of the Contracting States themselves to respect the relevant rights but must prevent or remedy any breach at subordinate levels.[49]

Best practice requires, at a minimum, the existence of internal rules regarding data collection and processing; the approval of highly intrusive data collection, such as surveillance operations, by an independent body, generally a judicial authority; the existence of effective civilian oversight bodies during and after law enforcement operations; the availability and dissemination of information about government personal data collection and processing; and the existence of effective and independent bodies able to provide remedies for the violation of the rights of targets, including judicial bodies.

For an oversight system to be effective, it is recommended to have at least six interdependent pillars of oversight and control, including:

- Internal oversight within law enforcement agencies;
- Executive control (policy control, financial control and horizontal oversight by government agencies);
- Parliamentary oversight (members of parliament, parliamentary commissions of inquiry);
- Judicial review;
- Oversight by independent bodies such as national human rights institutions, Ombudspersons, etc; and,
- Civil society oversight.[50]

49 *Assanidzé v Georgia* (71503/01) - judgment of 8 April 2004

50 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>

5.2 Effective Oversight Bodies

To be effective, oversight bodies must be able to initiate and conduct independent investigations, be adequately resourced in terms of budgets, expertise, material, and must have full and unhindered access to information, installations and officials.[51] For example, oversight bodies must have access to all relevant information, regardless of its level of classification, which they deem to be relevant to the fulfilment of their mandates. Access to information by oversight bodies should be enshrined in law that defines their mandates and powers. Any attempts to restrict oversight bodies' access to classified information should be prohibited and subject to sanction where appropriate. It may, however, be necessary to redact from public reports, information identifying potential targets, witnesses, and individual methods.

Law enforcement agencies have increasingly sophisticated capacities to collect, share and receive information and use increasingly complex systems for doing so. Accordingly, oversight bodies may require independent technical expertise to understand the functioning of various systems.

5.2.1 Independent Oversight Bodies

Independent oversight mechanisms" are autonomous from political, economic, military or other objectives. They have: 1) formal (*de jure*) independence requiring that they remain outside the bureaucratic, hierarchical chain of command within a ministry or other government agencies; and 2) actual (*de facto*) independence, which relates to the body's self-determination in conducting investigations and ensuring or recommending redress.[52]

5.3 Prior Independent Approval for Surveillance and Special Investigative Operations

The Human Rights Committee has established that the authorization of any 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.[53] The European Court of Human Rights has indicated that the authorizing body need not necessarily be a judicial body but such non-judicial body must be sufficiently independent from the executive. At the same time, the Court noted that 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. The Court also considered that although *ex-ante* authorization is not an absolute requirement *per se*, the *ex post facto* judicial review may not be sufficient in some circumstances, to counterbalance the shortcomings of the authorization and that *ex-ante* judicial authorization is therefore necessary.[54] This principle applies to both targeted and untargeted surveillance. Moreover, authorization must be grounded on facts. For example, the Inter-American Court of Human Rights expressed concerns about a domestic court having authorized

51 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>

52 See, for example, OECD Public Integrity Handbook Section 12.2.3, <https://www.oecd-ilibrary.org/sites/7715f0e0-en/index.html?itemId=/content/component/7715f0e0-en>

53 General Comment 16, para. 8.

54 Szabó and Vissy v. Hungary, para. 77.

surveillance despite the fact that the request for surveillance did not include any reasons or grounds to justify it. It also observed that those seeking surveillance permission had not indicated that less intrusive means of obtaining the information sought were unavailable.[55]

E*x ante* approval of particularly intrusive law enforcement operations must be received from an independent body before engaging in any of the following activities either directly or through/in collaboration with private sector entities:

- Conducting targeted surveillance measures, including the collection of and access to communications data (including when held by the private sector);
- Conducting untargeted bulk surveillance measures regardless of the methods or technology used or the type of communications targeted;
- Using selectors or key words to extract data from information collected through bulk surveillance, particularly when these selectors relate to identifiable persons;
- Collecting communications/metadata directly or accessing it through requests made to third parties, including private companies; and
- Undertaking computer network exploitation, a form of hacking.[56]

The European Court of Human Rights has addressed surveillance operations in a number of cases and the principles established are applicable to all forms of surveillance. Independent authorizations for surveillance must include:

- The details of individuals whose communications are to be surveilled;
- The nature of the offences justifying the intrusion;
- 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 and security of intercepted material; 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.[57]

The independent and effective body authorizing surveillance measures must also ensure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures.[58]

The same principles apply when law enforcement agencies seek personal data from the private sector.

55 k (2009), 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.

56 Council of Europe, Democratic and effective oversight of national security services, p. 12, available at: < https://book.coe.int/en/commissioner-for-human-rights/6682-pdf-democratic-and-effective-oversight-of-national-security-services.html>

57 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, footnote 687 citing ECtHR, Huvig v. France, Case no. 4/1989/164/220, 27 March 1990, paras. 32-33; ECtHR, *Kruslin v. France*, Application no. 11801/85, 24 April 1990, para. 35; ECtHR, *Greuter v. The Netherlands*, Application no. 40045/98, 19 March 2002.

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

5.3.1 Oversight During Operations and Ex-Post Review of Activities and Operations

The Human Rights Committee has noted that surveillance, interception, and hacking programmes can only be human rights compliant where robust and independent oversight mechanisms exist.[59]

The first degree of control in any police 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;
- 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.

The judiciary is an indispensable element of a police accountability system. Surveillance or covert data collection activities must be authorized by a judicial representative or body, or similarly independent mechanism, prior to the start of such activities, to the extent possible. In civil law systems, investigative judges monitor law enforcement activities while they are ongoing. And in all systems, the judiciary must be charged with adjudicating allegations of law enforcement 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 clear, precise, accessible, comprehensive and non-discriminatory legal frameworks on law enforcement surveillance programmes that are in line with international law, including international human rights norms and 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 surveillance programmes.

Some Member States have also established independent expert bodies, including but not limited to national human rights institutions, Ombudspersons, and/or data protection authorities authorised to oversee surveillance programmes. The precise form of such oversight bodies is not regulated by international law, but they must be independent and must have robust powers, including obtaining all information relating to full surveillance cycles, and make binding and public recommendations.

Oversight frameworks may integrate a combination of administrative, judicial and/or parliamentary oversight. Authorization and oversight bodies should be institutionally separated, although one judicial body may authorize an operation, and another may provide redress to victims.

Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and 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.[60] Oversight mechanisms may make recommendations

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

60 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>

for institutional and legislative reform that should be given appropriate consideration by the relevant executive and legislative bodies.

Oversight institutions must take all necessary measures to protect classified information and personal data to which they have access during the course of their work, and penalties imposed for the breach of these requirements by members of oversight institutions.[61]

5.4 Complaints Mechanisms

The existence of mechanisms to which individuals may challenge the lawfulness of alleged interferences with their human rights is fundamental and will enhance the development of principles of effective investigations. Victim involvement and public scrutiny have contributed to a growing awareness of the interests of data subjects. If public trust and confidence in the complaints system is to be secured and maintained, grievances must be adequately and proportionately addressed in accordance with the nature of the complaint.

Five principal types of police complaints mechanisms in operation around the world, include: internal police; Ministry for police or Interior; public prosecutor; ombudsman; civilian oversight. It is not uncommon for several mechanisms to operate in one jurisdiction.[62]

The establishment of an independent, external citizen oversight body with responsibilities for receiving and investigating complaints against the police is essential to achieve greater accountability and transparency and in some cases, to address shortcomings of ineffective internal control and oversight. A standard statutory purpose, in jurisdictions where police complaints systems have been codified, is to hold law enforcement officials accountable in criminal and disciplinary proceedings on the basis of evidence obtained in the investigation of a complaint. The same mechanisms that investigate allegations of the use of excess force by the police may also investigate allegations of unlawful interference with privacy or unlawful collection of personal online data, although the mechanism may require additional technical expertise. An effective police complaints system offers fundamental protection against the development of a culture of impunity. Additionally, complaints are an important resource that may be researched and analysed so that lessons may be learned from past mistakes for the purpose of improving future performance. Complaints provide lesson learning opportunities at the individual officer and service level.[63]

5.4.1 Remedy and Redress

Article 2 of the International Covenant on Civil and Political Rights establishes the right to an effective remedy for violations of human rights obligations.[64] Thus, individuals affected by the illegal actions of a law enforcement official or agency must have recourse to an institution that can provide an effective remedy, including full reparation for the

61 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. 14, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/134/10/PDF/G1013410.pdf?OpenElement>

62 Ibid.

63 Council of Europe, International Police Complaints Reform, available at: <https://rm.coe.int/16806dbbbd>

64 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; (c) To ensure that the competent authorities shall enforce such remedies when granted.

harm suffered. This may include non-judicial institutions empowered to receive and investigate complaints as well to issue binding orders or provide effective remedies, or judicial institutions that can order remedial action. To ensure the practical application of this right, states must ensure that individuals can also access an institution equipped to make legally binding orders about co-operation, including information that has been received from or sent to foreign bodies. The institutions responsible for addressing complaints and claims for effective remedy arising from the activities of intelligence services must be independent of law enforcement agencies and the executive branch. Such institutions must also have full and unhindered access to all relevant information, the necessary resources and expertise to conduct investigations, and the capacity to issue binding orders.[65]

5.4.2 Transparency

Transparency is critical in all democratic government operations. Therefore, 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.[66]

State authorities and oversight bodies should engage in public information about the existing laws, policies and practices in surveillance and communications interception and other forms of processing of personal data, as open debate and scrutiny are essential to understanding the advantages and limitations of surveillance techniques.[67]

Those who have been the subject of surveillance should be notified and have explained to them *ex post facto* the interference with their right to privacy if contemporaneous notification is not possible. Subjects should also be entitled to alter and/or delete irrelevant personal information, provided that information is inaccurate or no longer to necessary for purposes of a current or pending investigation.[68]

Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.[69] Oversight bodies should be required by law to publish public versions of their periodic and investigation reports. Additionally, law enforcement agencies and oversight bodies must not be generally exempt from freedom of information legislation. Instead, decisions not to make certain information public must be taken on a case-by-case basis, properly justified and subject to the supervision of an independent body.

65 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>

66 Principle 10. E of the Tshwane Principles on National Security and the Right to Information, available at: <https://www.justiceinitiative.org/publications/tshwane-principles-national-security-and-right-information-overview-15-points#:~:text=June%202013-,The%20Tshwane%20Principles%20on%20National%20Security%20and%20the%20Right%20to,and%20national%20law%20and%20practices.>

67 Report of the Special Rapporteur on the Right to Privacy, A/HRC/34/60, para. 38, available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement>

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

69 *Ibid.*, para. 40.

5.5 Commercially Aggregated Data

While international law requires that government agents obtain warrants or similar permissions, in compliance with clear, precise, accessible, comprehensive and non-discriminatory domestic law, before accessing individual personal data, the issue is complicated by the existence of commercially available data that aggregates publicly available and private information. Government agencies seeking to purchase data frequently use terms like 'open source' and 'publicly available' in their purchase orders and contracts, suggesting that they are only seeking information such as public social media posts that people knowingly make available to the public. However, government purchase orders and contracts frequently use these terms to include information collected specifically for a given agency that is not actually available to the public or any other consumer. The broad and misleading usage of these terms undermines governmental claims that agencies are permitted to collect such information on the basis that it is generally out there to the public and individuals, therefore, lack a reasonable expectation of privacy in such sensitive data.[70] At a minimum, where government agencies purchase data that includes, for example, financial or medical information, that a person would reasonably expect to be private, that data must be purchased in strict accordance with the principles set out in this report. Although outside of the scope of this document, the United Nations Guiding Principles on Business and Human Rights further details the obligations of States when they contract with business enterprises as well as the responsibility of such enterprises to respect human rights and to prevent and address all adverse human rights impacts directly linked to their operations, products or services.[71]

70 Center for Democracy and Technology, Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence agencies are Buying Your Data from Brokers, < https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/>

71 Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework | OHCHR. See also, Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital age, A/HRC/39/29, para. 42-49.

[VI] Summary of Considerations

6.1 Key Considerations

1. Member States must establish both internal and independent oversight mechanisms to monitor the activities of law enforcement officials with respect to online data collection and digital surveillance. Responsibility for oversight of online data collection and surveillance may be integrated into the duties of existing oversight mechanisms. Civilian oversight contributes to greater accountability and transparency.
2. External oversight mechanisms must be independent, properly resourced, and have full and unhindered access to all relevant information, premises and officials. They may include a mix of administrative, executive, legislative, and independent bodies, although the latter must have powers to investigate and provide effective remedy.
3. It is increasingly difficult to justify a distinction between the collection and processing of personal data and the collection and processing of metadata.
4. It is also difficult to create a legal distinction between government collection of personal data and the purchase of personal data from commercial entities.
5. The right to access personal data, and the circumstances in which such data may be accessed, must be established by clear, precise, accessible, comprehensive and non-discriminatory law or internal regulation and disseminated to all law enforcement officers. Violations of such rules must be addressed by existing or new disciplinary mechanisms.
6. In the interests of transparency, Governments must provide the population with information about their data collection and processing activities. To the extent possible, the operations and conclusions of oversight mechanisms must be made available to the public.
7. States must ensure that any victims of unlawful online data collection and surveillance can bring a complaint to an independent court or oversight institution and have recourse to an institution that can provide an effective remedy, including full reparation for the harm suffered.
8. Civil society is a key partner in the work to ensure human rights are respected in the collection and processing of personal data States are encouraged to create and maintain an enabling environment for civil society, including a legal framework that protects and promotes human rights, in accordance with international human rights law. They must ensure that any official impediments to civil society oversight of government collection and processing of personal data are subject to independent judicial review.

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)