August 2025

# Privacy International's submission to the UN Special Rapporteur on a Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism

## Introduction

Privacy International (PI) welcomes the call for inputs of the UN Special Rapporteur on counter-terrorism and human rights for a Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism.[1]

As a general remark, PI believes that the use of AI technologies in counter-terrorism poses significant risks to human rights, risks that in certain cases cannot be adequately mitigated. As a result, governments should not design or deploy AI technologies for counter-terrorism without having first demonstrated their capacity to comply with existing human rights law.

In the following sections, PI seeks to answer some of the questions posed in the call for inputs.

## How does the use of artificial intelligence (AI) in countering terrorism affect human rights? Which rights are impacted?

There are features of existing AI technologies, including when used in countering terrorism, that expand, intensify or incentivize interference with the right to privacy, most notably through increased collection, analysis and retention of personal data.

[1] Call for submission at https://www.ohchr.org/en/calls-for-input/2025/call-input-position-paper-human-rights-impacts-using-artificial-intelligence

As such, AI challenges the human rights to privacy, including data protection, in a variety of ways.

Firstly, with regards to data minimisation, AI systems typically rely on large data sets, often including personal data. This incentivizes widespread collection, storage and processing of vast amount of data.

Second, AI technologies may allow de-anonymization that is facilitated by fusing data from various sources. Personal data is defined as "any information relating to an identified or identifiable individual".[2] To assess whether a person is identifiable, one needs to look at the available technology. And with the development of AI, the capacity to identify individuals from seemingly anonymous data is increasing, as already noted by the UN High Commissioner for Human Rights in 2021.[3]

Arrangements enabling government agencies to have access to large data sets, including held by businesses, for example, increase the likelihood of identification and consequently of unlawful interference in the right to privacy, unless adequate safeguards are in place.[4]

Third, AI applications make inferences about individuals' characteristic and behaviours based on data. As such AI technologies challenge the distinction between categories of data, including personal data and sensitive personal data. Highly sensitive information can be inferred or predicted from non-sensitive types of data. For example, location data or browser searches can reveal individuals' religion or their sexual orientation. When sensitive personal data, such as information about race, ethnicity, or political beliefs can be predicted from unrelated data this poses significant challenges to the right to privacy.[5]

In the context of counter-terrorist measures, the processing of data by AI systems further amplifies risks of human rights abuses:

- the processing of vast amount of personal data in an indiscriminate and untargeted fashion raises concern of mass surveillance and questions about compliance with the principles of necessity and proportionality.
- the consequences of AI 'decisions' based on data processing can lead to serious interference with other human rights, such as right to liberty and freedom of movement. In counter-terrorism context, predictions, assessments and 'decisions' made by or with the support of AI technologies turn individuals into suspects, with significant consequences to their human rights. As noted by the UN High Commissioner for Human Rights, "AI assessments by themselves should not be seen as a basis for reasonable suspicion due to the probabilistic nature of the predictions."[6]

[2] See Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Article 2(a).

[3] U.N. Doc. A/HRC/48/31, para 14.

[4] See for example, PI, Bulk Personal Datasets & Bulk Communications Data challenge, https://privacyinternational.org/legal-action/bulk-personal-datasets-bulk-communications-data-challenge

[5] For some examples, see PI's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination, https://privacyinternational.org/advocacy/5295/pi-seeks-inform-report-ai-and-racial-discrimination-un-special-rapporteur-racism

[6] See U.N. doc: A/HRC/48/31, para 24.

- There are risks of exacerbating discriminatory practices, particularly when AI technologies are used to interpret data to predict future behaviours or infer characteristics on the basis of race, ethnicity, religion, etc. The discriminatory concerns of AI have been raised by UN human rights mechanisms. For example, the 2024 report of the UN Special rapporteur on contemporary forms of racism noted how AI systems supporting facial recognition technologies and predictive policing tools carry an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus of policing of certain groups.[7]
- AI technologies challenge the capacity to remain anonymous online and off-line, with serious implications for the rights to privacy, freedom of expression and peaceful assembly. The systematic collection of personal information even from public spaces is widely recognised as an inference with right to privacy. Yet this has been a long-standing practice without transparency, regulation or oversight.[8] AI systems are enabling intelligence and law enforcement authorities to collect and analyse the personal information of individuals which can be obtained from public spaces. This includes activities in physical spaces, for example via facial recognition technologies, and in digital spaces, particularly to track individuals on-line and to analyse data produced by social media interactions.

## Which specific applications of AI in efforts to counter terrorism pose the greatest risks to human rights?

- **Biometrics (including Facial Recognition Technologies)**

AI technologies are increasingly used to process biometric data (including facial images, via facial recognition technologies, FRT) for counter-terrorism purposes.

The processing of biometric data is encouraged by the UN Security Council resolutions, which impose legally binding obligations on all UN member states to develop biometric technologies for counter-terrorism purposes, paired with the strong promotion of these technologies by some, mostly Western states and by powerful industry players.

PI documented the human rights implications of the use of biometric technologies for counter-terrorism purposes and the use of AI technologies in this field. While the contexts vary from country to country, the main trends are very similar:

- The use of AI technologies to analyse biometric data in large, centralized databases, can seriously undermine the human right to privacy and have an irreversible impact on individuals. In this context, relatively fixed and unchangeable physical features – such as fingerprints and faces – are turned into machine-readable identifiers. Human rights experts are increasingly questioning whether some of these technologies, notably live facial recognition in public spaces, can ever be deployed in ways that do

[7] U.N. doc. A/HRC/56/68.

[8] U.N. doc: A/HRC/48/31. See also jurisprudence of the European Court of Human Rights, such as Case of Perry v. the United Kingdom, (Application no. 63737/00), 17 October 2003, https://hudoc.echr.coe.int/eng?i=001-61228

not violate the right to privacy and other human rights, such as freedom of peaceful assembly.

- There is a rising danger of "function creep", notably the gradual widening of a technology use beyond its original, intended purpose.
- AI technologies applied to biometric data can exacerbate exclusion and reproduce racial, ethnic, gender, social class, and other inequalities.
- The rapid deployment of AI technologies to process biometric data has not been met by commensurate changes at the level of law or policy in counter-terrorism context. National regulatory and legal frameworks continue to lag behind and, where they do exist, they are rarely effectively enforced, unable to properly safeguard against the hazards and potential misuses of biometrics. The 2021 CTED analytical brief on biometrics and counter-terrorism notes the inadequacy of national legal frameworks, including on data protection and oversight and accountability mechanisms, and states that legislation establishing safeguards "must be developed prior to the implementation of biometric systems".[9] Since then, little has changed. Attempts such as the EU AI Act to introduce prohibitions and limits to the use of AI for processing biometric data, including prohibiting live FRT by law enforcement agencies, are riddle with loopholes,[10] while in many other jurisdictions, including Brazil, Canada, China and the UK, regulation remains absent.[11]

- **SOCMINT**

Over the last few years, governments have been resorting to social media intelligence (SOCMINT) for counter-terrorism purposes.[12] In particular, social media monitoring is often justified as a form of content moderation for counter-terrorism purposes. It is also abused to surveil peaceful assemblies, measuring public sentiment and profiling people's social conduct.

Some of these activities are undertaken directly by government themselves, but in some instances, governments are calling on companies to provide them with the tools and/or knowhow to undertake this sort of surveillance.[13]

The type of personal information that is collected and analysed includes sensitive data revealing people's political opinion, religious belief, health conditions, sexual orientation and gender identity. As the OHCHR confirmed "social media intelligence ranges from the investigation of specific users to dragnet collection, storage and analysis of vast amounts of data."[14]

[9] CTED Analytical Brief on the use of biometrics in counter-terrorism, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf

[10] EDRi, EU's AI Act fails to set gold standard for human rights, https://edri.org/our-work/eu-ai-act-fails-to-set-gold-standard-for-human-rights/

[11] Matulionyte R, Zalnieriute M, eds. In: The Cambridge Handbook of Facial Recognition in the Modern State. Cambridge Law Handbooks. Cambridge University Press; 2024:i-ii.

[12] By SOCMINT we refer to the techniques and technologies that allow companies or governments to monitor social media networking sites.

[13] See Privacy International, Challenge against Clearview AI in Europe, https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe

[14] U.N. Doc. A/HRC/51/17, para 35.

Because of the sheer volume and complexity of such highly revealing data, various AI technologies are employed to analyse such data, including to profile users and to predict past, present and future behaviours.[15] Concerns about discrimination, reliability, false positive and false negatives of these AI based technologies have been raised by both the UN General Assembly and the UN Human Rights Council.[16]

Left unregulated, social media monitoring leads to the kind of abuses observed in other forms of covert surveillance operations. However, adequate national legal frameworks are largely missing in many countries.

- **Profiling in Military Decision-Making Systems**

With the blurring lines between law enforcement and military operations in the context of counter-terrorism,[17] AI-powered surveillance and targeting systems operated by the military are designed to identify, generate, and sometimes counter perceived terrorist threats. By analysing vast datasets for behavioural patterns or other indicators deemed suspicious, these systems designate individuals as potential threats and enable defensive responses to counter them. These systems, turn daily civilian lives into targets of suspicion and subject entire societies to scrutiny and control. By design, such systems cannot function without extensive surveillance infrastructures that continuously monitor entire populations. Only through this constant surveillance can they identify deviations from what is labelled “normal” behaviour. Recent developments highlight the dangers of this model. In Gaza, Israel reportedly used an AI system called Lavender to generate thousands of targeting recommendations based on a vast database of individuals. At one stage, the system flagged up to 37,000 people as potential targets due to perceived links with Hamas. These links were often based on broad and opaque criteria, which expanded or contracted depending on how the system was trained to interpret these relations.[18]

A similar logic underpins the rise of ‘deep sensing’, a new generation of military AI designed to gather, integrate, and analyse diverse data streams in real time to produce dynamic threat assessments. These systems draw from satellite imagery, drone footage, biometric data, and even social media activity, harvesting information across civilian and military environments alike. The goal is to create a “live” picture of the battlefield, but the implications are broader: entire populations risk being treated as data sources.[19]

[15] For more information and examples, see PI, Social Media Surveillance, https://privacyinternational.org/learn/social-media-surveillance

[16] UN Doc. A/RES/79/175 and UN Doc. A/HRC/RES/54/21. See also report of the Report of the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, UN Doc. A/HRC/56/68, paras 9-19.

[17] PI, ‘Challenging the Militarisation of Tech’, https://privacyinternational.org/campaigns/militarisation-of-tech

[18] The Guardian, The machine did it ‘coldly’: Israel used AI to identify 37,000 Hamas targets, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes)

[19] See Klaudia Klonowska & Sofie van der Maarel, ‘Deep Sensing, the New Military AI? Why Deep Sensing Should be on the Radar’, 6 May 2025, https://opiniojuris.org/2025/05/06/deep-sensing-the-new-military-ai-why-deep-sensing-should-be-on-the-radar/

## What key principles and safeguards should apply to the use of AI in countering terrorism to ensure the timely and effective protection of human rights?

Applying existing human rights standards can mitigate some of the risks posed by the use of AI for counter-terrorism.

Among the growing aquis related to human rights compliant use of technologies is the principle to refrain from or cease the use of AI technologies that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights, unless and until the adequate safeguards to protect human rights and fundamental freedoms are in place.[20]

The fact that AI is deployed for purposes of national security or defence should not void the human rights safeguards applicable to such technologies. In fact, given the enhanced human rights risks, it should lead to more stringent limits and controls. This need for responsible use of AI has been even acknowledged in various forums, including the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. While the Declaration has certain limitations, it contains a set of non-legally binding guidelines intended to promote best practices in military AI use. These "include ensuring that military AI systems are auditable, have explicit and well-defined uses, are subject to rigorous testing and evaluation across their lifecycle, have the ability to detect and avoid unintended behaviours, and that high-consequence applications undergo senior-level review."[21]

There are also certain specific safeguards that are key to ensuring the protection of the human right to privacy when designing and deploying AI technologies and that should thus be enshrined in law, implemented and enforced. Some of these safeguards[22] include:

- **Respecting human rights by design**

Decisions made in the design stage of AI application have a significant impact on whether the technology is human rights compliant. Relevant factors that would affect the design of an AI application include: deciding which processes will be automated; setting the values the AI application is designed to optimise; assessing the training data used; deciding in which circumstances the AI application shall be used.

Data protection legislation often includes obligations of privacy by design, requiring inter alia to ensure that the design of AI applications which process personal data limit data collection, restrict further data processing, prevent unnecessary and unauthorised access, amongst other privacy enhancing measures. These measures should all be part of the design of AI applications, but they should be complemented by considering other measures aimed at addressing other human rights risk factors. For example, testing and evaluation of AI

[20] UN Doc. A/RES/78/265, OP 5.

[21] Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, November 2023, https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/

[22] Other safeguards such as human rights impact assessments, independent oversight are mentioned elsewhere in this submission.

application should consider the specific context in which they are intended to be deployed; the data to be used in testing should allow to mitigate risks of bias and discriminatory outcomes. These requirements and safeguards should be built in laws that regulate AI technologies in the relevant sectors.

- **Ensuring adequate data security of AI technologies**

The security of the data, at rest and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data.[23] When assessing the level of security for AI applications, organizations should consider central processing and data storage sites, as well as the security of remote devices where data also may be collected or received. Security measures should include appropriate mechanisms for addressing actual and suspected security breaches.

- **Prevent discrimination and bias**

It is also essential to establish safeguards that prevent discrimination and algorithmic bias caused by the use of AI in counter-terrorism efforts. This includes conducting regular human rights impact assessments, implementing fairness-aware machine learning practices, and ensuring transparency in data selection and model design. Particular attention must be paid to the risk of disproportionate impacts on marginalised or vulnerable communities, in line with the principles of equality and non-discrimination under international human rights law.

## How do States and private entities' roles differ in their responsibilities with respect the design, development, acquisition, training and use of artificial intelligence in countering terrorism?

In the counter-terrorism context, government security and intelligence agencies and private companies often work hand in hand, and their roles and responsibilities in surveillance activities of individuals or population at large are often overlapping, ill-defined and opaque.

PI and its partners have documented several cases where police and security forces and other public authorities partner with private companies in order to expand their surveillance capabilities and process mass quantities of personal data, notably by deploying AI technologies.[24]

These public-private partnerships (PPPs) raise serious human rights questions regarding the involvement of private actors in the use of invasive surveillance technologies and the exercise of powers that have been traditionally understood as the states' prerogative.

These partnerships are taking on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the

[23] See PI, A Guide for Policy Engagement on Data Protection; The Keys to Data Protection, https://privacyinternational.org/sites/default/files/2018-09/Data Protection COMPLETE.pdf

[24] PI, Public-Private surveillance partnerships, https://privacyinternational.org/learn/public-private-surveillance-partnerships

state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services.[25]

There is a growing reliance by governments on the services offered by data analytics companies, which provide analytical techniques to search, aggregate, and cross-reference large data sets in order to develop intelligence and insights. While per se data analytics tools do not necessarily raise human rights concerns, the way they are used do so. PI has raised concerns about data analytics practices, by companies such as Palantir, whose tools may pose a real danger to people in vulnerable positions such as at international border crossings.[26]

PPPs should not operate in a legal vacuum. Widely recognised principles of human rights and good governance applicable to both governments and companies (notably via the UN Guiding Principles on Business and Human Rights) should apply, such as transparency, legality, necessity and proportionality, accountability, oversight, redress and proper procurement standards and procedures.[27]

## Do existing guidelines, legislation and regulatory mechanisms currently in place prove effective in ensuring humans exercise meaningful oversight over the use of artificial intelligence in operations countering terrorism? In addition to existing international initiatives to regulate and govern AI, is there a need for any dedicated mechanism(s) relating to AI in counter-terrorism specifically?

Due to the challenges that AI technologies pose (as noted above), there needs to be enhanced privacy safeguards throughout the AI lifecycle, if these technologies are included in counter-terrorism context.

Modern data protection laws – requiring inter alia an appropriate legal basis for any data processing, fairness and transparency, ensuring purpose limitation and data minimisation, accuracy, storage limitation, integrity and security, and accountability, as well as prohibition (with narrow exceptions) of solely automated decisions when such decisions have legal or other significant effects - should offer a good legal framework, applicable to any AI technology that process personal data, whether used by governments or private actors.

In practice, however, data protection laws are necessary but not sufficient to provide adequate protection. Firstly, despite improvements, national data protection legislation in a

[25] For up to date examples, see PI, Public-Private Surveillance Partnerships Tracker, https://privacyinternational.org/examples/public-private-partnership-tracker.

[26] See PI, Who supplies the data, analysis, and tech infrastructure to US immigration authorities?, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities

[27] For an overview of these principles, see PI, Safeguards for Public-Private Surveillance Partnerships, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

significant number of countries is inadequate, outdated, and lacking in effective enforcement. Secondly, general data protection legislation often does not apply (or apply in a limited ways) to processing of personal data for law enforcement or national security purposes, leaving a significant gap when it comes to use of AI for counter-terrorism purposes. Further, AI applications may rely on non-personal data to make or inform decisions that still negatively impact the human rights of individuals and groups affected. In these circumstances, data protection law offers little in ways of protection.

AI technologies cannot operate in a legal vacuum. Existing exemptions and loopholes to data protection legislation need addressing, before AI is deployed for counter-terrorism.

## How can due diligence processes, including human rights risk/impact assessments and mitigation measures, be effectively integrated into the lifecycle of AI technology development to better safeguard fundamental rights in the counter-terrorism context?

- **Human Rights Impact Assessment**

Human rights impact assessments of AI applications should be conducted at all stages of the AI lifecycle: prior to the design, during the development, the testing, the deployment and regularly thereafter in order to identify the emerging human rights risks. These assessments not only enable the identification of the risks and corresponding mitigation strategies required to respond to them, but they also provide a framework for deciding whether to go ahead with a particular AI technology.

For AI technologies for counter-terrorism purposes, PI believes that at a minimum, an impact assessment should include privacy and data protection impact assessments as well as an assessment of other human rights likely affected by the AI application as well as potential discriminatory effects. Measures should not be assessed in isolation, but should consider the cumulative effects of interacting measures. For example, before deciding to deploy new AI-based surveillance tools, a government must assess its existing surveillance capacities and their effects on the right to privacy and other rights. Such assessments should consider the necessity and proportionality of any interference with privacy or other human rights, the risks to individuals and groups, and how these risks are to be addressed and mitigated.

The assessments should be conducted with the participation of affected individuals and groups, civil society actors and independent experts. The outcome of the assessment should be made public and should detailed the mitigation and oversight measures envisaged. As noted by the Committee of Ministers of the Council of Europe “confidentiality considerations or trade secrets should not inhibit the implementation of effective human rights impact assessments.”[28]

[28] Council of Europe, Addressing the Impacts of Algorithms on Human Rights, Recommendation of the Committee of Ministers, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

The outcomes of the assessment could result in redesign but also in the cancellation if certain AI technologies cannot be deployed in a manner consistent with human rights.[29]

- **Independent oversight**

Any deployment of AI technology should be subject to independent, effective, adequately resourced and impartial oversight. Oversight should cover all parts of the design, use and throughout the deployment of AI application. Because of the human rights risk associated with the use of AI technologies for counter-terrorism, oversight should include judicial as well as parliamentary domestic oversight mechanisms capable of verifying the legality of the use of AI, ensuring transparency and accountability.

Oversight mechanisms must have the power and capacity to conduct regular auditing of AI applications to ensure their compliance with human rights and other standards. As noted by the UN Special Rapporteur on freedom of expression, protection of intellectual property and trade secrets cannot justify refusal of such oversight, particularly when the AI application is used by the public sector. Further, there are technical and policy options to address legitimate concerns related to proprietary technology, including allowing regulators and independent researchers access to AI applications on a confidential basis.[30]

## How should the explainability, foreseeability and transparency of AI systems be addressed?

The opacity of AI systems poses significant challenges to accountability and ultimately to access to effective remedies. However, not all sources of opacity are of a technical nature. This is particularly the case when opacity is due to proprietary software and trade secrets; deliberate opacity by design; or lack of technical expertise that is required to properly understand advanced processing using AI.

Data protection standards, such as the right to information, articulate some transparency requirements. Information shall include the category, purpose and sources of the data processed; the existence of profiling, of automated-decision making; and the logic involved and the significance and envisaged consequences of the processing. This may be elaborated further to include for example “factors taken into account for the decision-making process, and their respective ‘weight’ on an aggregate level” and how a profile was built “including any statistics used in the analysis”. Such an obligation should apply even where the task is burdensome. The domestic legal system, including intellectual property and trade secrecy, should not preclude transparency of AI applications. [31]

[29] U.N. Doc. A/RES/78/265, OP 5. See also report of the UN High Commissioner for Human Rights, which states: “A risk-proportionate approach to legislation and regulation will require the prohibition of certain AI technologies, applications or use cases, where they would create potential or actual impacts that are not justified under international human rights law, including those that fail the necessity and proportionality tests. Moreover, uses of AI that inherently conflict with the prohibition of discrimination should not be allowed.” U.N. Doc. A/HRC/48/31, para 45.

[30] See analysis and recommendations by the UN Special Rapporteur on freedom of expression, U.N. doc. A/73/348.

[31] As noted in the Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States of the Council of Europe on the human rights impacts of algorithmic systems: “the legislative frameworks for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose. Transparency levels should be as high as possible and proportionate to the severity of adverse human rights impacts,

Further, the principles of explainability and transparency of AI systems should continue to apply also in context related to security and countering terrorism. For example, while the US policies on AI are undergoing significant changes under the current administration, it is worth noting that already in 2020, the US Department of Defence five principles for the ethical development of artificial intelligence capabilities included explainability, stipulating that "AI should be designed in a way that allows relevant developers and users to adequately understand how the technology works (transparency) and be able to trace back sources of problems when something goes wrong (traceability). This can be achieved through the design of transparent and auditable methodologies, data sources, design procedures and documents."[32]

## Recommendations

Stemming from the points above, PI would like to suggest the following recommendations to be included in the Special Rapporteur's position paper on the use of Artificial Intelligence for counter-terrorism:

To states:

- refrain from or cease the use of artificial intelligence systems that are impossible to operate in compliance with international human rights law or that pose undue risks to the enjoyment of human rights;
- adopt and effectively enforce, through independent, impartial authorities, data protection legislation for the public and private actors developing and deploying AI in the context of counter-terrorism;
- develop and conduct human rights due diligence (including data protection impact assessment) prior to the design, development and deployment of any AI technologies for counter-terrorism purposes and regularly throughout the AI lifecycle in order to identify, prevent, mitigate and redress adverse human rights impacts;
- reinforce transparency of the use of AI technologies in counter-terrorism, including by adequately informing the public and affected individuals, enabling independent and external auditing of automated systems, and establishing effective remedies; and

including ethics labels or seals for algorithmic systems to enable users to navigate between systems. The use of algorithmic systems in decision-making processes that carry high risks to human rights should be subject to particularly high standards as regards the explainability of processes and outputs."
https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 Also Article 29 Data Protection Working Party, Guidelines on Automated Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN. WP 251rev.01, 6 February 2018, p 27. The Article 29 Working Party Guidance on Transparency (adopted by the European Data Protection Board) has underlined that "[…] the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default, transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle."
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[32] See DOD Adopts 5 Principles of Artificial Intelligence Ethics, https://www.defense.gov/News/News-Stories/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/

- ensure that, in the provision and use of AI technologies for counter-terrorism purposes, public-private partnerships uphold and expressly incorporate human rights standards.

To UN entities developing and supporting counter-terrorism policies:

- adhere to the UN Human Rights Due Diligence Policy when providing assistance in the use of AI technologies for counter-terrorism;
- develop, conduct and publish human rights risk assessments (including data protection impact assessment) prior to providing any assistance to Member States;
- regularly and meaningfully consult with national civil society organisations and experts during the prior human rights assessments and during the implementation of assistance programmes;
- strengthen the capacity to monitor Member States' compliance with human rights law, including data protection when using AI technologies for counter-terrorism;
- increase transparency and accountability of UN counter-terrorism programmes, including by publishing regular and granular reports on the activities carried to support Member States' capacity.