MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

Artificial Intelligence and Counter-Terrorism

Challenges and Chances for Human Rights

verfasst von / submitted by

Dr. Alrun Cohen-Soyer

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2022 / Vienna, 2022

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 891
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Human Rights (LL.M.)
Betreut von / Supervisor:	MMag. Dr. Ralph Janik, LL.M.

Artificial Intelligence and Counter-Terrorism

Challenges and Chances for Human Rights

Table of contents overview

Table of contents in detail

Abstract

(*for German see below*)

Logistics of terrorists have changed significantly. Communication channels have become more technically adept, letters and phones have been replaced by high-tech clandestine communication. The UN Security Council Counter Terrorism Committee notes a growing concern over the '*misuse of digital technologies*' by terrorists to commit, recruit for or plan attacks.

This development is accompanied by a new phenomenon of terrorism, *lone-wolf terrorism*: Persons who carry out attacks individually without being part of a terror organisation. However, they are hardly completely isolated, but radicalized and taught in online networks.

Intelligence agencies try to keep up with technological trends. They must quickly adapt their strategies, especially in information gathering. Social network surveillance has become an important area of counterterrorism. As the huge amount of data is impossible to be analysed by humans, authorities use a variety of Artificial Intelligence (AI) and algorithm-based tools to identify potential terrorists in advance. '*Predictive intelligence*' analyses personal data such as age, residence, education, family, friends and health of persons in order to identify suspects as well as patterns of groups. Algorithms detect keywords on social media linked to extremist ideologies. Eventually, automatic scoring systems measure the danger of a person and the risks of an attack, while being able to predict their place and timing and prepare a pre-decision.

Thereby AI is combined with *biometric methods*, a science concerned with measurements related to biological or behavioural human characteristics. For instance it collects and classifies fingerprints, iris scans or DNA and uses facial recognition, a tool to categorize persons based on their facial geometry as well as voice recognition to flag individuals who match terrorist profiles. Such data is highly sensitive, as a person can change their name, but not their DNA.

However, the high benefit of such methods is at the same time the core of their problematic nature. Their use is in tension with *fundamental rights*. While states must prevent terror attacks to protect their citizens' lives, they also have to protect the human rights of potential suspects. The thesis analyses the risks and chances of the use of AI. Are AI systems suitable for the use in counterterrorism and which legal safeguards must be observed? Which gaps in legal protection can be identified with regard to the collection, retention and processing of data? Thereby the thesis focusses on the European Convention on Human Rights and thus on the European Court of Human Rights' case law, in particular on the right to respect for private life (Art 8). Further, discriminatory outcomes of biased AI systems may violate the prohibition from

discrimination (Art 14). Of importance are also the right to an effective remedy (Art 13) and to a fair trial (Art 6), especially due to the lack of transparency. Since algorithms often are confidential, persons concerned might not even know *that* they have been identified by an algorithm, but even if so, the question *how* the algorithm has chosen them, stays in a *black box*, which hinders them to challenge the decision properly.

At the same time, the thesis analyses to what extent AI systems can bring *chances* with regard to the human rights protection of potential suspects. An important advantage of AI would be its ability to reveal existing discriminatory structures and *mitigate human bias in decision making*, if data is selected carefully. As algorithms can rapidly analyse large amounts of data, they can also help to predict who would be likely to support the same groups in the future, find similarities and correlations to the social environment and increase the *accuracy and precision of decisions*. Thereby, an intriguing question is, if AI can serve to deradicalize individuals? Through their ability of an early detection of group patterns as well as lone-wolf terrorist characteristics, algorithms can detect levels of *radicalization*. Some systems identify the susceptibility to violent extremist ideologies. For instance, the '*Redirect Method*' detects users of video-sharing sites that may be susceptible to the propaganda of terrorist groups and links them to another (positive) narrative. A great opportunity can be seen in this method.

Finally, based on the analysis of the ECtHR case law, the thesis develops proposals that attempt to reconcile the challenges and benefits of using AI in counterterrorism.

Abstract

Die Logistik von Terrorist:innen hat sich erheblich verändert. Kommunikationskanäle wurden technisch versierter, Briefe und Telefone wurden durch hoch technologisierte geheime Kommunikationsmittel ersetzt. Der Ausschuss für Terrorismusbekämpfung des UN-Sicherheitsrates stellt eine wachsende Besorgnis über den ‚*Missbrauch digitaler Technologien*' durch Terrorist:innen fest, um Anschläge zu begehen, für solche zu rekrutieren oder diese zu planen.

Diese Entwicklung geht einher mit einem neuen Phänomen des Terrorismus, dem sogenannten *einsamen Wolf Terrorismus*: dieser bezeichnet Personen, die alleine als Einzeltäter:innen Anschläge verüben, ohne Teil einer Terrororganisation zu sein. Allerdings sind sie kaum völlig isoliert, sondern werden in Online-Netzwerken radikalisiert und unterrichtet.

Die Geheimdienste versuchen den technologischen Trends nachzukommen. Sie müssen ihre Strategien rasch anpassen, vor allem bei der Informationsbeschaffung. Dadurch wurde die Überwachung sozialer Netzwerke zu einem wichtigen Bereich der Terrorismusbekämpfung. Da die riesigen Datenmengen nicht von Menschen ausgewertet werden können, nutzen Behörden eine Reihe von Instrumenten künstlicher Intelligenz (KI) und Algorithmen, um potenzielle Täter:innen im Voraus zu erkennen. Die ‚*prädiktive Analytik*' analysiert personenbezogene Daten wie Alter, Wohnort, Bildung, Familie, Freunde und Gesundheit von Personen, um Verdächtige sowie Gruppenmuster zu identifizieren. Algorithmen erkennen Schlüsselwörter in sozialen Medien, die mit extremistischen Ideologien assoziierbar sind. Schließlich messen automatische Bewertungssysteme die Gefährlichkeit einer Person und das Risiko eines Anschlags und sind in der Lage, Ort und Zeitpunkt vorherzusagen und eine Vorentscheidung zu treffen.

Dabei wird KI mit *biometrischen Methoden* kombiniert, einer Wissenschaft, die sich mit der Messung biologischer und verhaltensbezogener menschlicher Merkmale befasst. Sie erfasst und klassifiziert Fingerabdrücke, Iris-Scans oder DNA und nutzt etwa Gesichtserkennung, ein Instrument zur Kategorisierung von Personen anhand ihrer Gesichtsgeometrie sowie Stimmerkennung, um Personen zu kennzeichnen, die einem Terroristenprofil entsprechen. Solche Daten sind hoch sensibel, da eine Person zwar ihren Namen, nicht aber ihre DNA ändern kann.

In dem hohen Nutzen solcher Methoden liegt zugleich der Kern ihrer Problematik. Ihr Einsatz steht im Spannungsverhältnis mit *Grundrechten*. Während Staaten Terroranschläge verhindern müssen, um das Leben ihrer Bürger:innen zu schützen, müssen sie gleichermaßen die Menschenrechte potenzieller Verdächtiger wahren. Die Arbeit analysiert daher die Risiken und Chancen des Einsatzes von Künstlicher Intelligenz. Sind KI-Systeme für den Einsatz in der

Terrorismusbekämpfung geeignet und welche rechtlichen Garantien sind einzuhalten? Welche Rechtsschutzlücken sind in Bezug auf die Erhebung, Speicherung und Verarbeitung von Daten zu erkennen? Der Fokus liegt dabei auf der Europäischen Menschenrechtskonvention und damit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, insbesondere auf dem Recht auf Achtung des Privatlebens (Art. 8). Außerdem können diskriminierende Ergebnisse von KI-Systemen gegen das Diskriminierungsverbot (Art. 14) verstoßen. Von Bedeutung sind auch das Recht auf einen wirksamen Rechtsbehelf (Art. 13) und auf ein faires Verfahren (Art. 6), vor allem wegen fehlender Transparenz. Da Algorithmen oft vertraulich sind, wissen die Betroffenen möglicherweise nicht einmal, *dass* sie von einem Algorithmus identifiziert wurden, aber selbst wenn, bleibt die Frage, *wie* der Algorithmus sie ausgewählt hat, Teil einer *Blackbox*, was sie daran hindert, die Entscheidung angemessen zu bekämpfen.

Gleichzeitig untersucht die Arbeit, inwieweit KI-Systeme *Chancen* im Hinblick auf den Schutz der Menschenrechte potenzieller Verdächtiger mit sich bringen können. Ein wichtiger Vorteil der KI ist ihre Fähigkeit, bestehende diskriminierende Strukturen aufzudecken und eine Voreingenommenheit in der Entscheidungsfindung durch Menschen abzuschwächen, wenn die Daten sorgfältig ausgewählt werden. Da Algorithmen dazu fähig sind, rasch große Datenmengen zu analysieren, können sie auch dazu beitragen, vorauszusagen, welche Personen in Zukunft wahrscheinlich dieselben Gruppen unterstützen werden, Ähnlichkeiten und Korrelationen zum sozialen Umfeld finden und die Genauigkeit und Präzision von Entscheidungen erhöhen. Dabei stellt sich die spannende Frage, ob KI dazu dienen kann, Personen zu deradikalisieren? Durch ihre Fähigkeit zur frühzeitigen Erkennung von Eigenschaften sowohl von Gruppenmustern als auch terroristischer Einzelgänger, können Algorithmen den Grad der Radikalisierung erkennen. Einige Systeme erkennen die Geneigtheit zu gewalttätigen extremistischen Ideologien. Beispielsweise erkennt die ‚*Redirect-Methode*' Nutzer von Video-Sharing-Seiten, die für die Propaganda terroristischer Gruppen anfällig sind, und verbindet sie mit einem anderen (positiven) Narrativ. In dieser Methode kann eine große Chance gesehen werden.

Schließlich werden auf der Grundlage der Analyse der Rechtsprechung des EGMR Vorschläge entwickelt, die den Versuch wagen, die Herausforderungen und Vorteile des Einsatzes von KI in der Terrorismusbekämpfung miteinander in Einklang zu bringen.

I. List of Abbreviations

AI	Artificial Intelligence
AI HLEG	European Commission's High-Level Expert Group on Artificial Intelligence
CERD	Committee on the Elimination of Racial Discrimination
CFR	Charter of Fundamental Rights of the European Union (2000)
Convention 108+	Council of Europe Convention for the protection of individuals with regard to the processing of personal data (2018)[1]
CTC	United Nations Security Council Counter-Terrorism Committee
CTED	United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTC and CTED both also 'UN Counter-Terrorism Committee')
ECHR	European Convention on Human Rights (1950) (also 'the Convention')
ECtHR	European Court of Human Rights (also 'the Court')
FRA	European Union Agency for Fundamental Rights
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
HRC	Human Rights Council
HRCttee	Human Rights Committee
ICCPR	International Covenant on Civil and Political Rights (1976)
NLP	Natural language processing
OHCHR	The Office of UN High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
SNA	Social network analysis
UN Office of Counter-Terrorism	United Nations Office of Counter-Terrorism, established 15 June 2017

[1] Council of Europe, Convention for the protection of individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981 (Convention 108) and its 2001 Additional Protocol related to transborder data flows to non-parties to Convention 108 and the mandatory establishment of national data protection supervisory authorities and transborder data flows, CETS No. 181, 2001; in its 128th session, 18 May 2018, the Committee of Ministers, Elsinore, amended Protocol CETS No. 223 for the modernisation of Convention 108 (Convention for the protection of individuals with regard to the processing of personal data "Convention 108+" (2018).

II. Outline - What do AI, lone wolves and Intelligence have in common?

1. Since 9/11…

The War on Terror and the aftermath of the 9/11 attacks increased the demand for data analytics significantly. Intelligence agencies failed in predicting the attacks as they lacked information that pointed to the terrorist organization of 9/11.[2] The subsequent invasion of Iraq was justified on the grounds that weapons of mass destruction would exist, which turned out to be a miscalculation.[3] In 2005, a report of a special Commission addressed to the President of the United States, stated '*that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction. This was a major intelligence failure. Its principal causes were the Intelligence Community's inability to collect good information about Iraq's WMD programs, serious errors in analyzing what information it could gather, and a failure to make clear just how much of its analysis was based on assumptions, rather than good evidence*.'[4] As a result, doubts grew about the analytical capabilities of human intelligence.[5] The question arose whether rational, automated control systems would be less prone to error.

In addition, the increase of data sets due to the Internet demands new systematic and automated data analysis. Terrorists make advantage of the speed in technological advances. Likewise, of course, the intelligence work and surveillance methods became highly complex.[6] Since 9/11 EU Member States also increasingly use *digital* intelligence methods. Not only the use of biometric data through methods such as facial or voice recognition, iris scan, DNA or fingerprints[7] but also the collection, retention and analysis of communications and digital data containing personal information have become common methods.[8] Eventually also the nature of terrorism has taken a new form, as will be highlighted in the next point.

---

[2] Damien Van Puyvelde, Stephen Coulthart, M. Shahriar Hossain, 'Beyond the Buzzword: big data and national security decision-making' (2017) 1398.
[3] Laurence H. Silberman, Charles S. Robb, 'The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction' (2005), 2.
[4] Laurence H. Silberman/Charles S. Robb, 'The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction' (2005), 2.
[5] Damien Van Puyvelde et al., 'Beyond the Buzzword: big data and national security decision-making' (2017) 1398.
[6] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 9.
[7] Krisztina Huszti-Orbán/Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?' - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism (2020) 8.
[8] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 17.

2. Phenomena of the Zeitgeist - new technologies and 'lone wolf' terrorists

Two phenomena form the premises of this thesis:

1) *New technologies*: Logistics of terrorists have changed the speed and range of attacks.[9] Today's communication channels have become more extensive and technically adept, from letters and phones to high-tech, often clandestine communication.[10] In the context of terrorism, the European Court of Human Rights recognises that modern means and changes in (tele-)communication behaviour '*require that investigative tools for law enforcement and national security agencies be adapted*'.[11] Similarly, the UN Security Council Counter Terrorism Committee (CTC) notes a growing concern over the '*misuse of digital technologies*' by terrorists to commit, incite, recruit for, fund or plan terrorist acts.[12] This development is accompanied by a new phenomenon of terrorism:

2) *Lone-wolf terrorism*: Terrorism is not only carried out by groups, organisations and networks but also by attackers who plot their attack by themselves individually.[13] This type of terrorism is growing rapidly.[14] The emergence of lone-wolf terrorism is linked to the trend of terrorism increasingly turning to social networks:[15] Recent attacks have been carried out by individual actors who have radicalized themselves via social media, unnoticed by intelligence agencies. However, even though committing an attack alone, they are usually not completely isolated. Many lone-wolf attackers '*are recruited, radicalized, taught, trained, and directed by others. They connect, communicate, and share information, know-how, and guidance exclusively online, through the "Dark Web*."'.[16]

---

[9] United Nations Office of Counter-Terrorism, Algorithms and Terrorism: The malicious use of Artificial Intelligence for terrorist purposes (2021) 19.
[10] United Nations Office of Counter-Terrorism, Algorithms and Terrorism: The malicious use of Artificial Intelligence for terrorist purposes (2021) 20.
[11] *Breyer v. Germany* App no. 50001/12 (ECtHR 30 January 2020) para 88; similarly already in 2008 with regards to techniques of identification such as DNA: *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 105.
[12] Office of Counter-Terrorism, Cybersecurity source: https://www.un.org/counterterrorism/cybersecurity (accessed 15th April 2022).
[13] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014) (https://medium.com/p/17b12f8c455a - accessed 9.7.2022).
[14] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014); Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 14.
[15] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 14.
[16] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014).

Lone wolf attackers in particular are said to experience a sense of social alienation, while the social network intervenes in this void and serves as a virtual community for them.[17] Online they can find everything they need from motivational speeches to information about targets and guidelines how to build a bomb.

By way of example, the last week of March 2022 was overshadowed in Israel by three terrorist attacks of lone actors.[18] In the third attack the assailant used an assault rifle shooting at civilians in several locations.[19] This attack is reminiscent of the terrorist attack in November 2020 in Vienna, when an attacker shot people indiscriminately with an automatic long gun in the old town.[20] Similarly, Dzhokhar and Tamerlan Tsarnaev, two brothers who allegedly carried out the bombing attacks at the Boston Marathon in April 2013, were not members of any terrorist organization and are seen as '*self-taught'*, '*unaffiliated with any particular terrorist group*' and '*fuelled by the web'*.[21] According to FBI investigations, they were motivated by extremist Islamic beliefs primarily through social media[22] and the online magazine 'Inspire', published by Al-Qaeda members, and were coached in building bombs.[23] On Facebook before the attack, Tamerlan had posted links to videos of fighters in the Syrian civil war and to Islamic websites with titles such as: '*There is no God but Allah, let that ring out in our hearts*.'[24] According to the Global Terrorism Index 2022, religious terrorism has been the deadliest form of terrorism in the West over the past ten years, in

[17] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014).
[18] Hadas Gold, Five people shot dead near Tel Aviv, the third attack in Israel in a week, CNN (published 30.3.2022), https://edition.cnn.com/2022/03/29/middleeast/shooting-near-tel-aviv-intl/index.html ; Amos Harel, Second Terror Attack in a Week Reflects Israeli Intel's Shortcomings (published 28.3.2022), https://www.haaretz.com/israel-news/.premium.HIGHLIGHT-after-terror-attack-israel-needs-to-figure-out-if-this-is-part-of-something-bigger-1.10702333 (accessed 30.3.2022).
[19] Hadas Gold, Five people shot dead near Tel Aviv, the third attack in Israel in a week, CNN (30.3.2022).
[20] LPD Wien, Aktueller Ermittlungsstand rund um den Terror-Anschlag am 2. November 2020 in Wien (published 13.11.2020), https://www.bmi.gv.at/news.aspx?id=2F4F4D5758556B416D79633D .
[21] Michael Cooper/Michael S. Schmidt/Eric Schmitt, Boston Suspects Are Seen as Self-Taught and Fueled by Web (23.4.2013), https://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html .
[22] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014).
[23] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014); Caitlin Dewey, Al-Qaeda's Inspire magazine celebrates Boston bombings, *The Washington Post* (published 31.5.2013) (https://www.washingtonpost.com/news/worldviews/wp/2013/05/31/al-qaedas-inspire-magazine-celebrates-boston-bombings/ - accessed 9.7.2022); Richard Valdmanis, Boston bomb suspect influenced by Al Qaeda: expert witness, *Reuters* (published 23.3.2015) (https://www.reuters.com/article/us-boston-bombings-trial-idUSKBN0MJ0Z620150323 - accessed 9.7.2022); generally about the magazine Inspire also Mark D. Chang, 'Trolling new media: violent extremist groups recruiting through social media', Calhoun: The NPS Institutional Archive (2015) 42.
[24] Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014).

particular in the form of radical Islamist terrorism.[25] Groups or lone actors inspired by Jihadist organisations are allegedly responsible for 528 deaths in the West since 2007.[26] Thereby social media functions a loophole; terrorists use social media for recruitment and propaganda, as counterterrorism authorities have blocked traditional websites and also because social media makes a large audience easily accessible.[27]

3. Why there is a need to use algorithm-based tools and AI to combat terrorism?

These lone-wolf attacks share the fact that the attackers were not sufficiently recognized by intelligence and were apparently unnoticed to prepare the attack beforehand. A major problem is that since they act alone, they are not easily identifiable in advance by traditional intelligence methods, which is why their attacks are '*seemingly impossible to defend against*'.[28] Intelligence agencies are far behind the technological trends. They must quickly adapt their counterterrorism strategies to the new nature of terrorism, especially in information gathering. Social network surveillance has therefore become an important area of counterterrorism.[29]

After Israel experienced its terrorism wave between 2015 and 2017, cyber specialists started to develop technical tools to detect potential attackers in advance.[30] According to a study led by the Ministry of Public Security of Israel, based on 700 attackers, at least 95 published their intent on social media indicating prior to the attacks.[31] So following the first wave, Law enforcement intelligence started to use new technologies to monitor social media content in order to identify potential attackers and patterns and prevent terrorist attacks.[32]

In the case of the terrorist attack of Vienna in November 2020, human errors played a major role. According to the report of an ad hoc Investigative Commission,[33] the responsible

---

[25] Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 33 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[26] Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 33 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[27] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 14; Daniel Byman, Terrorism and the threat to democracy, Brookings Policy Brief (February 2019) 5.
[28] Daniel L. Byman, Why lone wolves fail (published 16.6.2016), https://www.brookings.edu/blog/order-from-chaos/2016/06/16/why-lone-wolves-fail/ ; 'Lone wolf' terror attacks hard to stop, says security expert, The Guardian https://www.theguardian.com/uk-news/2015/dec/06/lone-wolf-terror-attacks-impossible-to-stop-says-security-expert .
[29] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 14.
[30] International Institute for Counter-Terrorism, IDC Herzliya, „A New Study on Lone Wolf Terrorism in Israel" (published 26.6.2018) https://www.ict.org.il/Article/2221/Lone_Wolf_Terrorism_Israel#gsc.tab=0 .
[31] Ministry of Public Security of Israel, „Study: Terrorists post info on social media before attacking" (published 12.6.2018) https://www.gov.il/en/Departments/news/study_on_lone_wolf_terror_phenomena_120618 .
[32] Marwa Fatafta, Algorithms of Occupation: Use of Artificial Intelligence in Israel and Palestine in Jonathan Andrew, Frederic Bernard (Ed.) Human Rights Responsibilites in the Digital Age (2021) 83.
[33] Ingeborg Zerbes et al, Untersuchungskommission zum Terroranschlag vom 02.11.2020, Geschäftszahl BMI: 2020-0.748.397 (10.2.2021) https://www.bmi.gv.at/downloads/Endbericht.pdf .

employees of the State Office for the Protection of the Constitution in Vienna misjudged key warning signals regarding the attacker that '*clearly indicate his dangerousness*'[34]; among them, in particular his participation in a meeting with other persons, whereby this was placed in the context of an IS terror cell and was announced by the German Federal Criminal Police Office, as well as the perpetrator's attempt to purchase ammunition for military weapons only one day later. Both facts were known to investigators, but were not deemed sufficiently dangerous. Would have algorithm-based tools measured the danger more accurately?

4. Which tools are used to combat terrorism?

Law enforcement authorities use a variety of Artificial Intelligence (AI) and algorithm-based tools to identify potential terrorists in advance.[35] Many military systems use AI for the analysis of the huge amount of the collected data,[36] as "predictive intelligence"[37] to analyse personal data such as age, residence, education, family, friends and health of persons in order to identify suspects,[38] but also predict place and timing of attacks[39]. Some systems even recognize and assess susceptibility to violent extremist ideologies, including, f.i., the '*Redirect Method*', which detects users of video-sharing sites that may be susceptible to the propaganda of terrorist groups and links them to another (positive) narrative (see also Chapters IV.1. and VIII.4.).[40] Frequently these tools include automatic scoring systems, which measure the dangerousness of

---

[34] Ingeborg Zerbes et al, Untersuchungskommission zum Terroranschlag vom 02.11.2020 (2021) 18.

[35] An algorithm is a set of instructions, a coded recipe that gets executed when it encounters a trigger, while AI is a group of algorithms that can „learn", so it can modify and create new algorithms based on new input data, which is described as "intelligence": Reinhard Klaushofer, Die menschenrechtliche Dimension Künstlicher Intelligenz, ZÖR 74 (2019) 407; Kaya Ismail, AI vs. Algorithms: What's the Difference?, CMS Wire (published 26.10.2018), https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/(accessed 23.7.2022).

[36] Maggie Gray, Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.

[37] Michaela Wiegel, Eines der weitreichendsten Anti-Terror-Gesetze der EU https://www.faz.net/aktuell/politik/ausland/frankreich-setzt-im-anti-terror-kampf-auf-algorithmen-17464470.html ; Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism, The Royal Institute of International Affairs (2019) 8; Marwa Fatafta, Algorithms of Occupation: Use of Artificial Intelligence in Israel and Palestine in Jonathan Andrew/Frederic Bernard (Ed.) Human Rights Responsibilites in the Digital Age (2021) 83.

[38] Among the source, the research for the design of the AI tool is based on, some of the sources are also regarding Israeli military, because they specificly had to deal with new challenges of the „lone wolf" terrorists. However, For the case study it will be assumed that the tools are used in **Europe to combat terrorism.** This is in fact also the case: Dan Williams, „Europe Looks Towards Israel for Anti-terror Technology", Haaretz (published 19.7.2016) https://www.haaretz.com/israel-news/europe-looks-towards-israel-for-anti-terror-technology-1.5412900 (accessed 30.3.2022).

[39] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 9; Report by the Islamic Military Counter Terrorism, Artificial Intelligence and Counterterrorism Limitations, Opportunities and Risks (2020) 3; Maggie Gray, Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.

[40] Report by the Islamic Military Counter Terrorism, AI and Counterterrorism Limitations (2020) 3.

a person and the risks of an attack and eventually prepare an automated decision.[41] The key is that only a large amount of data is suitable for identifying meaningful patterns; at the same time, such an amount of data can only be evaluated efficiently by machine analysis. In addition, there has been an increase of special researchers who look for key words linked to extremist ideologies on social media. In order to understand the terrorist's motivation and to identify patterns, psychologists attend interrogations.[42] This thesis will focus especially on techniques related to data analytics and thus not f.i. on AI related autonomous weapons.[43]

AI tools are often combined with *biometric methods*, a science concerned with measurements and metrics related to biological or behavioural human characteristics.[44] As the UN Counter-Terrorism Committee recently noted, as new technologies, such as highly sensitive cameras, algorithms and AI linked to databases, develop increasingly, so does the use of biometrics in counterterrorism.[45] Therefore several variants – such as the collection and classification of fingerprints, facial recognition, a tool to categorize persons based on their facial geometry, sometimes hidden as drones[46], voice recognition, iris scans or DNA – are being used to flag individuals who match terrorist profiles.[47] By using facial recognition, closed-circuit television might even monitor entire public places.[48] US defence agencies have recently even developed a tool which is able to identify persons based on their 'heart print'.[49] A person can change their name, but they can't change their biometrical data, which makes this data particularly sensitive. Eventually, technological tools are often combined with human intelligence.

---

[41] Eric Tlozek, Israel is using an algorithm to spot the next 'lone wolf terrorist', and soon other countries will too, abcnews (published 21.12.2018) https://www.abc.net.au/news/2018-12-22/israel-algorithm-to-predict-next-palestinian-lone-wolf-terrorist/10620900 (accessed 30.3.2022).

[42] Marwa Fatafta, Algorithms of Occupation: Use of Artificial Intelligence in Israel and Palestine in Jonathan Andrew/Frederic Bernard (Ed.) Human Rights Responsibilites in the Digital Age (2021) 83.

[43] For this see Maggie Gray, Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.

[44] Krisztina 5.

[45] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 2.

[46] United Nations Office of Counter-Terrorism, Algorithms and Terrorism (2021) 34.

[47] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 8; Marwa Fatafta, Algorithms of Occupation (2021) 83; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism (2020) 4.

[48] United Nations Office of Counter-Terrorism, Algorithms and Terrorism (2021) 42.

[49] Heartbeat patterns are distinctive enough to allow for the identification of a person. See Dave Simonds, The Economist, 'People Can Now Be Identified at a Distance by Their Heartbeat', (published 23.1.2020) https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat (accessed 30.3.2022).

5. Impact on Human Rights

However terrorism has always had a '*twofold effect*' on human rights law:[50] On the one hand states must protect the life and physical as well as mental integrity of their citizens and therefore try to prevent terror attacks. However, on the other hand, they have to protect the human and fundamental rights of potential suspects and perpetrators. Possible violations, as analysed in Chapter VII, may concern the right to life, the prohibition of torture, inhumane or degrading treatment or punishment, the right to security of the person, to fair trial and an effective remedy and – with regard to the focus of the thesis – in particular the right to respect for private and family life. A particular issue is transparency. Since the use of the algorithm often is held confidential, suspects might not even know that they have been identified by an algorithm, but even if so, the algorithm itself is not disclosed to them; it stays a „*black box*".[51] However, without appropriate information, they cannot challenge the algorithm and identify gaps.

As early as 2014, the Office of the United Nations High Commissioner for Human Rights (OHCHR) stated its concern that 'examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure'.[52] This development led to the consequence that – at least in Western countries – fundamental freedoms were restricted for the entire population, justified with the aim to prevent terrorist attacks.[53] According to a recent study by the Fundamental Rights Agency, the surveillance of individuals is in principle regulated in detail in almost all EU Member States, but only five Member States have detailed legislation on the interception of communications.[54] However, the legal framework is highly complex in all 28 member states, not to mention countries outside the EU, such as the U.S. or Israel. A common criticism is the diversity, unpredictability, and ambiguity in the legal field of AI use, most notably in the area of counterterrorism operations.[55]

Recently, the UN Counter-Terrorism Committee noted a huge increase in surveillance on social media and in the use of biometric data for purposes of counter-terrorism. However, the

---

[50] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 7.
[51] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism 17; Janneke Gerards/Raphaële Yenidis, Algorithmic discrimination in Europe (2020) 10; Human Rights Council, UNHCR Report (A/HRC/48/31) para 20, 56; FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 35.
[52] OHCHR, Human Rights Council, 27th session, A/HRC/27/37 (2014), The right to privacy in the digital age, 3.
[53] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 42.
[54] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 9.
[55] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 9.

Committee simultaneously criticizes insufficient legal bases and the lack of effective remedies.[56] Taking facial recognition as an example, in 2020 the CERD emphasised its impact on discrimination saying that racial profiling '*is committed by law enforcement authorities and is not motivated by objective criteria or reasonable justification*'.[57] This may include border checks, home searches, targeting for surveillance, while these actions may take place in the context of anti-terrorism operations.[58] Biases in the systems itself may lead to over-criminalization of certain groups of people.[59] There has been an increase of this issue due to '*rapid advances in technological development*' as '*actions of law enforcement officials are determined or informed by algorithmic profiling, which may include big data, automated decision-making and artificial intelligence tools and methods*'.[60] Thereby the CERD notes the lack of effective remedies and redress tools, and at the same time a vicious circle as a negative consequence is the: people affected by discriminatory law enforcement tend to trust the authorities less and therefore cooperate less, limiting the effectiveness of law enforcement.[61] One year later, in 2021, the Committee of Convention 108+ published Guidelines on Facial Recognition including a limitation by law of its use,[62] the necessity of supervisory authorities[63] and the importance of the high quality of techniques thereby addressing the developers;[64] similar Guidelines were published in 2022 by the European Data Protection Board.[65]

More recently, the COVID-19 pandemic has made pre-existing risks related to conspiracy theories and hate speech more transparent than ever before.[66] This, of course, increases the dangers of radicalization, especially with regard to easily seduced individuals. However, at the same time, the relevance of human rights protection increased due to the Covid situation. During the pandemic, measures to monitor the population were stepped up, for example to be able

[56] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 4 f.
[57] Committee on the Elimination of Racial Discrimination General recommendation No. 36, CERD/C/GC/36, 'Preventing and Combating Racial Profiling by Law Enforcement Officials' (24 November 2020) para 13.
[58] *Ibid.* para 19.
[59] *Ibid.* para 30.
[60] *Ibid.* para 31.
[61] *Ibid.* para 26.
[62] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 6.
[63] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 8.
[64] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 9.
[65] European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement - Version 1.0' (12 May 2022).
[66] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 43.

to check compliance with quarantine regulations.[67] On the one hand, this allowed masses of data to be collected, while, at the same time, the threshold for the interference into the privacy sphere was also gradually lowered. There is a correlation between the rapid development of new technical tools to combat the pandemic and the use of such data to fight crime. The restrictions on movement also explain why the COVID-19 pandemic has led to a decline of terrorism.[68] However, the Global Terrorism Index 2022 fear an increase in terrorist activity after the end of the pandemic because extremists would take advantage of resentment over restrictions, economic issues, health policy issues and vaccination obligations.[69]

Against this background, the thesis focusses also on the state's responsibilities to combat terrorism and the opportunities of AI and algorithm systems. In order to protect lives the state can be even obliged to collect data of terror suspects. According to a study by the Ministry of Public Security of Israel predictive intelligence monitoring social media managed to decrease the terrorism wave between 2015 and 2017 which was carried out by lone actors.[70] One focus is therefore on how the new technologies can be used to benefit the protection of the population and (inter)national security, while equally taking into account the respect for human rights.

6. Research Questions and Scope of the Thesis

This thesis examines the following questions:

1) *Are AI systems suitable for the use in counterterrorism while complying with human rights?*
2) *What legal criteria and safeguards are to be considered based on the ECtHR case law?*
3) *Which gaps in legal protection are apparent based on the ECtHR case law?*
4) *Can AI systems bring benefits with regard to the human rights protection of suspects?*
5) *To what extent can AI systems be used for deradicalization of individuals who are easily seduced into extremism?*

Thereby the thesis limits its analysis to the human rights and fundamental freedoms enshrined in the European Convention on Human Rights. As the right to respect for private life is the most relevant right with regard to the use of AI technologies and data protection, the thesis will focus

[67] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 19 f.
[68] Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 14 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[69] Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 14 f – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[70] Ministry of Public Security of Israel, 'Study: Terrorists post info on social media before attacking' (12.6.2018).

in particular on Article 8 ECHR. Discriminatory outcomes whose decision-making processes are not comprehensible due to a lack of transparency could violate the prohibition from discrimination (Article 14 ECHR). Of great importance is also the right to an effective remedy, so emphasis will be placed on the analysis of Article 13 ECHR. Particularly in the use of artificial intelligence in the legal field - in the legislature, but especially in the judiciary and the executive branch - the highest sensitivity to bias must be maintained. Since it is also a relevant procedural guarantee, the rights under Article 6 ECHR are highlighted next. Other rights affected, but with limited specific issues arising in relation to AI, include (but are not limited to) the right to life (Article 2 ECHR), the prohibition of torture (Article 3 ECHR) and the rights to freedom of thought, expression, religion, and assembly (Articles 9-11 ECHR). Thereby the whole process concerns several stages, collection, retention, processing and sharing data,[71] while at each level a Human Rights assessment should be made.

III. Definitions

1. Artificial Intelligence and Algorithm

1.1. Artificial Intelligence ("AI")

Artificial intelligence ('AI') is a group of algorithms able to learn, meaning that it can modify and create new algorithms based on new input data and carry out cognitive or perceptual functions, described as 'intelligence'.[72] Their main function in the field of counter-terrorism is their ability to identify patterns.[73] The thesis will be based on the AI's definition of the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG):[74]

'Artificial intelligence (AI) systems are software (and … hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their

[71] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 14.
[72] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 8; Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 407.
[73] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 16 f.
[74] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 6.

environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.'

AI includes several techniques, such as machine learning (see 1.2. 'deep learning'), machine reasoning (which includes planning, knowledge, reasoning, optimizing), and robotics (which includes control, sensors, integration of all other techniques into cyber-physical systems).[75] The starting point of AI is information, which is incorporated in various ways, be it through data inputs, cameras, microphones, sensors and the like. All the information collected will be transformed into data, i.e. codes, so that the system can process it.[76] The special feature of AI is the ability to evaluate and weight this information in order to arrive at specific decisions with regard to the objective.[77] The process is characterized by codes and algorithms that vary from system to system. At the end and the core of the AI process lies its reasoning and autonomous decision making ability and this in addition in unbelievable speed.[78] Therefore, AI is often used in predictive algorithm-based decision-making processes ('predictive analytics').[79] This methodology is used, for example, to analyse the future purchasing behaviour of customers[80] or - relevant here - to identify potential future terrorists and attacks in advance. While AI systems (only) modify their environment, they do not adapt or improve their own behaviour.[81]

1.2.Deep Learning

A separate category is *'deep learning'*, characterized by its ability to independently improve their capabilities without human intervention based on the functioning of the human brain.[82]

---

[75] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 6.
[76] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 406.
[77] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 8; Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 406; Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 7.
[78] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 2 f.
[79] Österreichischer Rat für Robotik und Künstliche Intelligenz (2018) 47 f.
[80] Österreichischer Rat für Robotik und Künstliche Intelligenz (2018) 48.
[81] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 3.
[82] Stefan Luber, Nico Litzel, 'Was ist Deep Learning?', Big Data Insider, (published 26.4.2017) (https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/ - accessed 6.7.2022); United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 18.

Thus, these systems can improve their own behaviour and adapt its own methods.[83] As a result, the system may become so autonomous at a certain point that it already acts and decides according to its own criteria, which may no longer be comprehensible to the originators.[84]

1.3.Algorithm

In contrast to AI, an '*algorithm'* is a set of rules or instructions, comparable to a coded recipe which gets executed when it encounters a trigger[85] and functions to solve a problem. Usually algorithms are set in computers, however, also a human could follow an algorithmic process, such as by using a mathematical formula to solve an equation.[86]

1.4.Big Data

Algorithms and AI systems are fed with data. '*Data*' itself is information, contained in a set of values of variables about persons, either qualitative (e.g. education) or quantitative (e.g. age).[87] One main challenge in the field of terrorism, is, however, the large amounts of data.[88] Terms as '*Big data*' or '*big data datasets'* usually refer to vast amounts of quantitative data, which can be used to discover dangers and reveal patterns by applying an algorithm.[89] They can be of different types (e.g., numbers, words, pictures) and intended for a specific purpose or general and unspecific,[90] whereas the latter could be sensitive from a human rights perspective.

---

[83] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 3.
[84] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 407.
[85] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 407; Kaya Ismail, AI vs. Algorithms: What's the Difference?, CMS Wire (published 26.10.2018), https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/ (accessed 21.7.2022).
[86] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 8.
[87] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 17.
[88] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 17.
[89] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 8.
[90] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 8.

1.5.NLP and SNA

Natural language processing (NLP) is a part of AI and enables machine learning technologies, computers, to *understand* language the same way as humans do.[91] It is used, for instance, to understand and analyse written postings on social media automatically.[92]

Social network analysis (SNA) is a comprehensive method for understanding the behaviour of actors and the network structures they are part of and use.[93] The method can be applied to real-world social networks (such as now in the context of the Covid pandemic) or to online networks, especially social media. To do this, technical mathematical formulas are used to encode the networks and link them to "nodes."[94] The method is used to classify the actors within the group, detect clustering, and predict individual or group behaviour.

2. The Definition of 'terrorism'

Since the thesis focuses on counter-terrorism, the first question is: What is terrorism? While there are 'countless definitions'[95], there is still no acknowledged definition of 'terrorism' as such in international law.[96] In general, however, terrorism can be understood as the '*resort to ideologically-, ethnically-, or religiously-motivated severe violence against individuals or property with the aim of coercing key social actors such as governments, international organizations, or transnational corporations into certain actions or omissions by causing deep and widespread fear.*'[97]

The Rome Statute does not include 'terrorism' as a separate crime. However, a terrorist act might constitute a crime against humanity (Article 7), defined as one of the therein listed acts such as murder '*when committed as part of a widespread or systematic attack directed*

---

[91] Ben Lutkevich, 'natural language processing (NLP)', SearchEnterpriseAI https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP (accessed 27.7.222); United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 20.

[92] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24; see https://www.insiktintelligence.com (accessed 26.7.2022).

[93] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 21.

[94] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 21: 'A fundamental step for analyzing social networks is to encode network data into low-dimensional representations, typically using a set of nodes to represent individual elements of the network and a set of links or edges between these nodes which correspond to pairwise relations'.

[95] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 6.

[96] Human Rights Council A/HRC/49/45 (Follow-up report on the Joint Study (2010) on Global Practices in Relation to Secret Detention in the Context of Countering Terrorism - Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism): The report speaks of the 'lack of a globally agreed definition of terrorism and (violent) extremism'.

[97] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 1.

against any civilian population with knowledge of the attack' or it might as well fall under its Article 8 as an indiscriminate attack against civilians or hostage taking.[98]

In a broader sense, 'terrorism' according to Article 2 lit b of the International Convention for the Suppression of the Financing of Terrorism[99] includes any '*act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act*.'

International institutions, in order to determine their mandate and measures, also tried to develop definitions. One of the most important was created in 1994 by the General Assembly's Declaration on Measures to Eliminate International Terrorism in its resolution 49/60 according to which terrorism includes '*criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes" and that such acts "are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them*.' In 2004, the Security Council in the resolution 1566 (2004) nearly identically continued with this definition while adding that the criminal acts committed have the '*intent to cause death or serious bodily injury, or taking of hostages*' and to '*intimidate a population or compel a government or an international organization to do or to abstain from doing any act*'.[100] The Special Rapporteur on Human Rights notes that the '*terminology*' in the resolution 1566 (2004) seems to have been interpreted by States as '*de minimis threshold*'. At the same time, he points out that broader domestic definitions may accordingly lead to a wide scope of application. The problem with this, he says, is that it would interpret the mandate of Council resolutions too broadly, taking action beyond what can legitimately be described as a threat to interstate peace and security and, ultimately, beyond what the Council intended.[101]

The lack of a definition is problematic from a human rights perspective. In particular, it is necessary to define 'terrorism' in order to determine the variety of measures which may apply

[98] Office of the United Nations High Commissioner for Human Rights, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet Nr. 32 (2008) 14 f.
[99] International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.
[100] Security Council, resolution S/RES/1566 (2004), para 3.
[101] In the 73rd General Assembly, A/73/361 (Advancing human rights through the mainstreaming of human rights in counter-terrorism capacity-building and technical assistance at the national, regional and global levels) para 34.

to ‘counter-terrorism’. In order to discuss the following questions under a common denominator, the thesis will be based on the definition by Martin Scheinin, former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:[102] Accordingly, terrorism means an action or attempted action where:

‘1. The action:

(a) Constituted the intentional taking of hostages; or

(b) is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or

(c) involved lethal or serious physical violence against one or more members of the general population or segments of it;

and

2. The action is done or attempted with the intention of:

(a) provoking a state of terror in the general public or a segment of it; or

(b) Compelling a Government or international organization to do or abstain from doing something;

and

(3) The action corresponds to:

(a) The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or

(b) all elements of a serious crime defined by national law.’[103]

On this basis, the thesis understands counter-terrorism as a common term for legal activities which are intended to prevent terrorist acts in the sense of the above description.

IV. Application of AI in the field of terrorism

Terrorist attacks in liberal democracies aim to destroy the values of democracy and undermine popular support for the government and the state. One goal of terror is to unsettle society as a whole, and an important element of this is unpredictability. Attacks seemingly coming out of

[102] Human Rights Council, 16th Session (22/12/2010) A/HRC/16/51, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin - Ten areas of best practices in countering terrorism (Dec 2010) para 28: ‘Practice 7. Model definition of terrorism’.
[103] Human Rights Council, 16th Session (22/12/2010) A/HRC/16/51, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin - Ten areas of best practices in countering terrorism (Dec 2010) para 28: ‘Practice 7. Model definition of terrorism’.

nowhere create deep insecurity in society. Therefore, even more than in the case of attacks directed against individuals, the focus in counterterrorism is on prevention.[104] Two methods have always proven effective: *deterrence*, for example by imposing heavy penalties, and the prevention of attacks in the first place by *identifying* the perpetrators and their intentions before they carry out their acts. In other words, it is a matter of recognizing the radicalization tendencies of future terrorists.[105] This can be realized through the use of predictive intelligence.

1. Predictive intelligence

Law enforcement authorities, intelligence and military systems use AI and algorithm-based tools for the analysis of the huge amount of data[106] to identify potential terrorists in advance. Usually, the purpose of the usage of AI systems and algorithms is to identify criminal characteristics both in terms of potential perpetrators and attacks. The algorithm can be used either before the collection of data or in order to collect data. In the latter case, criminological information can be automatically collected and stored in databases.[107]

The term of the method '*predictive intelligence*'[108] summarizes techniques used in order to identify suspects but also predict place and timing of attacks.[109] Some systems even assess the impact of general factors, such as the country's economic and political situation, on the risks of terrorist attacks.[110] In an earlier stage, the '*Redirect Method*'[111] is a fascinating tool to detect individuals who may be susceptible to propaganda from terrorist groups. Its automated system

---

[104] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 5.
[105] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 5.
[106] Maggie Gray/Amy Ertan, 'Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment' (2021), 19.
[107] Nikolay Radulov, 'Artificial Intelligence and Security. Security 4.0.', International Scientific Journal "Security & Future" 2019, 4; see f.i. Chris Baraniuk, 'Durham Police AI to help with custody decisions', BBC, 10.5.2017 (https://www.bbc.com/news/technology-39857645 - accessed 8.7.2022); Bernard Marr, How Robots, IoT And Artificial Intelligence Are Transforming The Police, *Forbes*, (published 19.9.2017) (https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/?sh=50710b485d61 - accessed 8.7.2022).
[108] Michaela Wiegel, Eines der weitreichendsten Anti-Terror-Gesetze der EU https://www.faz.net/aktuell/politik/ausland/frankreich-setzt-im-anti-terror-kampf-auf-algorithmen-17464470.html ; Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism, The Royal Institute of International Affairs (2019) 8; Marwa Fatafta, Algorithms of Occupation: Use of Artificial Intelligence in Israel and Palestine in Jonathan Andrew/Frederic Bernard (Ed.) Human Rights Responsibilites in the Digital Age (2021) 83.
[109] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 9; Report by the Islamic Military Counter Terrorism, Artificial Intelligence and Counterterrorism Limitations, Opportunities and Risks (2020) 3; Maggie Gray/Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.
[110] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 9 f.
[111] Jigsaw (2016). 'The Redirect Method', www.redirectmethod.org (accessed 19.7.2022).

targets users of video-sharing sites and redirects them to videos providing a credible counter-narrative.[112] Frequently these tools include automatic scoring systems, which measure the dangerousness of a person and the risks of an attack and eventually prepare an automated decision.[113] The present thesis will focus especially on techniques related to data analysing methods and thus not f.i. on autonomous vehicles and autonomous weapons by applying AI.[114]

2. Types of methods

2.1. Data Analytics

Automated data analysis is used to support executive and intelligence agencies. In particular, AI systems based on predictive intelligence are used to analyse personal data such as age, residence, education, family, friends and health of persons in order to identify potential suspects but also predict place and timing of attacks.[115] In this way, individual persons, patterns but also terrorist networks are to be recognized and detected and activities prevented in advance.[116] For example, since the 9/11 attacks, there has been an increase to assess the risk of airline passengers.[117] AI systems match elements of passenger name records for all travellers with terrorist and law enforcement databases to find possible matches or to perceive secondary signals as alerts, e.g., if a passenger had reported his passport's loss just before the flight.[118]

---

[112] Report by the Islamic Military Counter Terrorism, AI and Counterterrorism Limitations (2020) 3; Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 10.

[113] Eric Tlozek, Israel is using an algorithm to spot the next 'lone wolf terrorist', and soon other countries will too, abcnews (publ. 21.12.2018).

[114] For this see Maggie Gray/Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.

[115] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 9; Report by the Islamic Military Counter Terrorism, Artificial Intelligence and Counterterrorism Limitations, Opportunities and Risks (2020) 3; Maggie Gray/Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021), 19.

[116] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 8.

[117] Bart Elias, 'Risk-Based Approaches to Airline Passenger Screening, Congressional Research Service Report', (2014) 7 with reference to the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458).

[118] Bart Elias, 'Risk-Based Approaches to Airline Passenger Screening, Congressional Research Service Report', (2014) 9 f.

2.2.Biometric data

Another field of methods are biometrics, a science concerned with measurements and metrics related to biological or behavioural human characteristics.[119] Therefore several variants – such as the collection and classification of fingerprints,[120] facial recognition, voice recognition, iris scans or the analysis of DNA codes[121] – are being used to flag individuals who match terrorist profiles.[122] By using facial recognition closed-circuit television might even monitor entire public places.[123] US defence agencies have recently even developed a tool which is able to identify persons based on their '*heart print'*, because according to studies heartbeat patterns are distinctive enough to allow for the identification of a person.[124] However, the sensitivity is obvious; a person can change their name and data of home address, but they cannot change their biometrical data, which makes this data in particular sensitive. The sensitivity is also related to the fact that biometric data are often misused by dictatorial regimes (e.g. Nazi regime or genocide in Rwanda) for - apparent - determination of an ethnicity.[125] This makes control and protection against misuse all the more important. Biometrics are especially used in border controls to verify persons' identities and identify potential suspects by quick checking (international) databases such as INTERPOL.[126] In some cases, the competence of intelligence includes the collection of biometric data itself, in others it is limited to accessing government databases;[127] but what they have in common is the authority to view such data and to use their analysis.

---

[119] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 1; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 5.
[120] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 1; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 4.
[121] Nikolay Radulov, 'Artificial Intelligence and Security. Security 4.0.', International Scientific Journal "Security & Future" 2019, 5; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 4.
[122] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 8; Marwa Fatafta, Algorithms of Occupation (2021) 83; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 5.
[123] United Nations Office of Counter-Terrorism, Algorithms and Terrorism (2021) 42.
[124] Dave Simonds, 'People Can Now Be Identified at a Distance by Their Heartbeat', *The Economist* (published 23.1.2020) https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat (accessed 9.7.2022).
[125] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 6.
[126] INTERPOL, 'Preventing Terrorist Travel', https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel (accessed 11.7.2022).
[127] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 9.

One commonly used method is *face recognition*, a tool to categorize persons based on their facial geometry, sometimes hidden as drones.[128] The ability to automatically capture and assign images of people in databases facilitates the identification of (potential) perpetrators.[129] However, facial recognition may prevent citizens from exercising their freedoms of assembly and association, as they are not anonymous anymore and it could as well interfere with their interest to be informed and consent in the storage of personal data.[130]

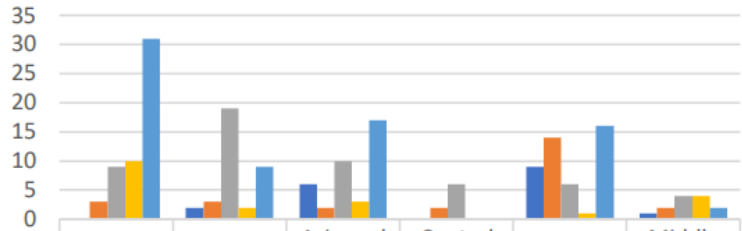
Similarly, *voice recognition* systems, familiar in the form of Amazon's Alexa, are capable of identifying a person solely on the basis of their voice. This method is therefore also used by intelligence services and the police. For example, the algorithm could trigger an alarm when it recognizes the voice of a known.[131] For instance, the voice identification system currently used by the National Security Agency (NSA) uses keywords to automatically search for recordings and identify potential terrorists, which replaces an infinite number of human investigators who would have to listen to the huge amount of recordings.[132]

According to a study of the UN Counter-Terrorism Committee of 2021, States are expanding the range of digital spaces (social media) where they are validating biometric data and are increasingly developing terrorist watch lists and databases linked to biometric databases.[133]

---

[128] United Nations Office of Counter-Terrorism, Algorithms and Terrorism (2021) 34; Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 4.
[129] Nikolay Radulov, 'Artificial Intelligence and Security. Security 4.0.', International Scientific Journal "Security & Future" 2019, 5.
[130] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 16.
[131] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 26 f.
[132] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 27.
[133] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 4.

Table 2: States using biometrics in counter-terrorism (as of 30 November 2021)



	Africa	Americas	Asia and Pacific	Central Asia	Europe	Middle East
Yes	0	2	6	0	9	1
Largely	3	3	2	2	14	2
Partially	9	19	10	6	6	4
Marginally	10	2	3	0	1	4
No/ Insufficient information	31	9	17	0	16	2

Source: UN Counter-Terrorism Committee[134]

2.3.Scanning social networks

As terrorist organizations such as Al-Qaeda or ISIS nowadays use Social Media to recruit perpetrators, law enforcement and intelligence are now using AI systems to monitor and analyse Social Media to prevent such recruitment attempts and detect radicalization before it occurs.

According to a study by *Weimann*, terrorist groups have moved their online presence to social media networks such as Facebook, Twitter, Instagram and YouTube and in the year of 2014 already '*90 percent of terrorist activity on the Internet takes place using social networking tools*'.[135] One of the reasons is that many Websites founded after 9/11 have been investigated by the intelligence services which prompted terrorist groups and organisations to turn to social media.[136] Unlike usual Websites, social media enables any person to access, create, publish and discuss information.[137] Purposes for using social media is the easy access to promote propaganda and thereby radicalize and recruit sympathizers.[138]

---

[134] CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021) 4.
[135] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 1 by referring to cyberterrorism expert Evan Kohlmann; see also Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 28.
[136] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 2.
[137] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 2.
[138] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 2; Azizan, Sofea Azrina, and Izatdin Abdul Aziz Aziz, Terrorism Detection Based on Sentiment Analysis Using Machine Learning', Journal of Engineering and Applied Sciences 12 (2017/3) 691, 692.

As of September 2012, *Facebook* had an estimated 1 billion,[139] as of January 2014 1.3 billion[140] and as of April 2022 already 2,9 billion[141] users around the world. This becomes relevant for terrorist organisations. In a jihadi online forum calling for 'Facebook Invasion' it was emphasised that '*if you have a group of 5,000 people, with the press of a button you [can] send them a standardized message. (…) Let's start distributing Islamic jihadi publications, posts, articles, and pictures*.'[142] Twitter is also increasingly used by terrorists and sympathizers, in particular to spread propaganda content as well as to communicate in real time among each other.[143] In a similar way, YouTube[144], Instagram and Flickr[145] are being used by terrorist groups to disseminate their propaganda videos and pictures for purposes of radicalization.

Therefore an increasingly important application of AI is *social network scanning* to find individuals who may have become radicalized or who intend to radicalize others.[146] Predictive AI methods can, for instance, use sentiments towards *keywords* typically linked to terrorism such as 'bomb', 'ISIS' or 'Hisbollah'.[147] As successful examples, the British home office claims that by using a specific algorithm ('ML') they were able to detect 94% Islamic State (ISIS) propaganda videos with 99.995% accuracy (precision) [148] and Facebook claims that 99% of Al Qaeda and ISIS posts are detected by machine learning before a user flags the post.[149]

---

[139] Mark D. Chang, 'Trolling new media: violent extremist groups recruiting through social media', Calhoun: The NPS Institutional Archive (2015) 22.
[140] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 4.
[141] Facebook Statistics and Trends, *Datareportal* (https://datareportal.com/essential-facebook-stats#:~:text=Facebook%20had%202.936%20billion%20monthly,'active'%20social%20media%20platforms – accessed 9.7.2022).
[142] This website (https://news.siteintelgroup.com/index.php/19-jihadist-news/1462-jihadist-gives-analysis-of-electronic-jihad) is not accessible any more, quoted after Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 5.
[143] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 8 f; Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 29; Azizan, Sofea Azrina, and Izatdin Abdul Aziz Aziz. 2017. "Terrorism Detection Based on Sentiment Analysis Using Machine Learning." Journal of Engineering and Applied Sciences 12 (3), 691, 692; Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015), https://arxiv.org/pdf/1503.02401.pdf (accessed 27.7.2022).
[144] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 11.
[145] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 13.
[146] Nikolay Radulov, 'Artificial Intelligence and Security. Security 4.0.', International Scientific Journal "Security & Future" 2019, 5.
[147] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 28; Azizan, Sofea Azrina, and Izatdin Abdul Aziz Aziz. 2017. "Terrorism Detection Based on Sentiment Analysis Using Machine Learning." Journal of Engineering and Applied Sciences 12 (3), 691, 692.
[148] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 29.
[149] Josh Horwitz, "Facebook Says It Can Stop the Sharing of Most Terror-Related Posts within an Hour of Creation." Quartz, 29.11.2017, https://qz.com/1140539/facebook-says-its-able-tostop-the-sharing-of-most-isis-terror-posts-withinan-hour-of-creation/ (accessed 21.7.2022).

V. Recent Developments

As a response to the 9/11 attacks, the United Nations Security Council adopted resolution 1373 (2001) on 28 September 2001, which obliges the Member States under Chapter VII of the Charter to take measures in order to prevent "*the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents*."[150] Further, it requires the Member States to report regularly to the Counter-Terrorism Committee on their progress.[151] In several resolutions, the Security Council urges states to implement national counterterrorism measures only in accordance with international human rights law, refugee law, and humanitarian law.[152]

Over the past decade, several attempts have been made to develop legal guidelines at the intersection of counter-terrorism and new technologies. In 2010, the Human Rights Council published the '*Compilation of good practices on legal and institutional frameworks and measures*' (UN Good practices) aiming to ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight.[153] This set of soft law standards is the only encompassing document on this topic at universal level.

In 2012, the OSCE placed a strategic paper for their future activities on countering terrorism.[154] Among other activities, it focusses on promoting the implementation of an international legal framework against terrorism and enhancing international legal co-operation in terrorism matters, countering violent extremism and radicalization that lead to terrorism and countering the use of the Internet for terrorist purposes, while at the same time, promoting and protecting human rights and fundamental freedoms in the context of counter-terrorism measures.[155]

Only two years later the Security Council issued Resolution 2178 (2014)[156]. Its background was the observation, that – as a result of ISIL/Da'esh's loss of control over territories also – terrorist

---

[150] S/RES/1373 (2001), adopted on 28 September 2001, para 2 (g).
[151] S/RES/1373 (2001), adopted on 28 September 2001, para 3 (6).
[152] See UN Security Council resolutions S/RES/1373 (2001), adopted on 28 September 2001, § 3 (f), resolution 1456 (2003), Annex, para. 6 and resolution 1624 (2005), para. 4.
[153] UN, Human Rights Council A/HRC/14/46 (2010), Report of the Special Rapporteur Martin Scheinin.
[154] OSCE Consolidated Framework for the Fight against Terrorism, PC.DEC/1063, Decision No. 1063, 934th Plenary Meeting (7 December 2012).
[155] OSCE Consolidated Framework for the Fight against Terrorism, PC.DEC/1063, Decision No. 1063, 934th Plenary Meeting (7 December 2012) Annex, 5.
[156] S/RES/2178 (2014), adopted by the Security Council at its 7272nd meeting, on 24 September 2014; see also Fionnuala Ní Aoláin, 'The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law', Just Security, 17 January 2018, available at https://www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/ (accessed 21.7.2022).

networks changed tactics and decentralized. Resolution 2178 (2014)[157] therefore addresses the growing threat posed '*foreign terrorist terrorists*', defined as '*individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict, and resolving to address this threat'*.[158]

The Resolution 2178 (2014) expresses their concern about the increasing use of communications technologies, especially the Internet, by terrorists and their supporters to radicalize for extremist ideas and recruit for terrorist acts. Member states would need to cooperate to prevent terrorists from exploiting technology and resources, while '*respecting human rights and fundamental freedoms and in compliance with other obligations under international law'*.[159]

Security Council resolution 2396[160] is of particular importance here. First of all, it focuses on improving border security, strengthening efforts to '*prosecute, rehabilitate, and reintegrate*' foreign terrorists and improving coordination within the UN counterterrorism structure in its support to the Member States. The main – new – aspect, however, are binding obligations for the Member States to develop *biometric* capabilities. Prior to this Resolution, such an obligation had not yet been established under international law.[161] According to para 15, the MS '*shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law*'. Further, Resolution 2396 also requires Member States to *develop watch lists or databases* of known and suspected terrorists, including foreign terrorist fighters (para 13). They shall serve for law enforcement agencies, military and intelligence agencies as well as border security and customs to screen travellers and make risk assessments and investigations, in compliance with domestic and international law, including human rights law (para 13). Further the Resolution 2396 encourages Member States to share this information through bilateral and multilateral mechanisms (para 13).

---

[157] S/RES/2178 (2014), adopted by the Security Council at its 7272nd meeting, on 24 September 2014; see also Fionnuala Ní Aoláin, 'The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law', Just Security, 17 January 2018, available at https://www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/ (accessed 21.7.2022).
[158] S/RES/2178 (2014) § 6.
[159] S/RES/2178 (2014) § 11.
[160] Resolution S/RES/2396 (2017), adopted by the Security Council at its 8148th meeting, on 21 December 2017.
[161] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 11.

Eventually, in March 2020 NATO's Science and Technology Organization[162] recognized that AI might have a '*revolutionary'* impact on NATO operations and in October 2021, NATO adopted an '*AI Strategy*' to cooperate '*among Allies on any matters relating to AI for transatlantic defence and security*'.[163] One of the expressed goals is to encourage responsible development and use of AI for Allied defence and security purposes, whereby integrating AI into military systems. And finally, on a more general level, in June 2021, the United Nations General Assembly affirmed[164] the United Nations Counter-Terrorism Strategy,[165] which encourages all Member States to address the threat posed by the increasing influx of recruits to terrorist organizations, including by implementing commitments to the use of biometric data while fully respecting human rights and fundamental freedoms.

VI. Legal Frameworks

The following section focuses on the European regional system and thus on the European Convention on Human Rights and the case law of the European Court of Human Rights (see II.6).

For the interpretation of the concerned rights, Convention 108+[166] also plays a role. It is an international treaty and a legally binding commitment of the Council of Europe member states to protect the right to privacy of individuals. It is not a closed document and some non–Council of Europe states have acceded to the treaty, respectively: Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, and Uruguay.[167] Since its adoption, Convention 108 has undergone a few rounds of updates. An additional Protocol was adopted in 2001 to bring the Convention 108 in line with the Data Protection Directive from 1995. The Convention was again updated in 2018 to align with the GDPR in what is known as Convention 108+, however it is drafted in a more accessible language and manner than the highly legalistic GDPR.[168] The

---

[162] NATO Science and Technology Organization, 'Science and Technology Trends 2020–2040: Exploring the S&T Edge' 14.
[163] Maggie Gray, Amy Ertan, 'Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment' (2021), 13; the Strategy itself is not published, but a summary: https://www.nato.int/cps/en/natohq/official_texts_187617.htm .
[164] A/RES/75/291.
[165] A/RES/60/288.
[166] Council of Europe, Convention for the protection of individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981 (Convention 108) and its 2001 Additional Protocol related to transborder data flows to non-parties to Convention 108 and the mandatory establishment of national data protection supervisory authorities and transborder data flows, CETS No. 181, 2001; in its 128th session, 18 May 2018, the Committee of Ministers, Elsinore, amended Protocol CETS No. 223 for the modernisation of Convention 108 (Convention for the protection of individuals with regard to the processing of personal data "Convention 108+" (2018).
[167] Collin J. Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection. Why Canada Should Consider Accession', CIGI Papers No. 246 (November 2020) 2.
[168] Collin J. Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection. Why Canada Should Consider Accession', CIGI Papers No. 246 (November 2020) 1 ff.

main purpose of this Convention is '*to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him*' (Article 1).

The new Convention 108+ includes an exception to the protection of personal data for the processing activities for national security. It aims to address privacy challenges from new technologies and strengthen enforcement.[169] When acceding to Convention 108+, a country undertakes the obligation to implement a law with the principles and mechanisms for enforcement required by Convention 108+.[170] However, the Convention 108+ itself does not have a complaint mechanism for persons concerned. That is the difference to the European Convention on Human Rights which offers the jurisdiction of the European Court of Human Rights (after the exhaustion of remedies under the domestic law, Article 35 of the Convention).

Under the General Data Protection Regulation (GDPR), any processing and collection of personal data amounts to interference. This could play a role in the following ways: Intelligence services are able to collect data from suspects indirectly, namely by collecting from telecommunication providers of their customers. However, as the GDPR is directed at states and not directly at individuals, the thesis does not focus on this legal instrument.

VII. Challenges for Human Rights

1. From the state's perspective

Before addressing the potential interference with the rights of the suspect, however it is essential to highlight the dangers of terrorism. Against this background, restrictions on human rights of terrorist suspects become more comprehensible. Finally, work in the field of counterterrorism must attempt to strike a balance between the interests of protecting citizens from terror and guaranteeing that terror suspects are treated in accordance with human rights.

From the perspective of the state, terrorism threatens many fundamental rights and freedoms of the civilian population. Terrorism aims to attack confidence in the fundamental values of democracy and the rule of law. Terrorist acts can destabilize governments, thereby threatening peace and security both nationally and internationally, and also have a negative impact on social

[169] Collin J. Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection. Why Canada Should Consider Accession', CIGI Papers No. 246 (November 2020) 3.
[170] Graham Greenleaf, 'RENEWING DATA PROTECTION CONVENTION 108: THE COE'S 'GDPR LITE' INITIATIVES', (2016) 142 Privacy Laws & Business International Report, 14-17 August (2017) 7.

and economic development. The destructive impact of terrorism on human rights has been recognized by several institutions such as the Human Rights Council, the General Assembly, the Security Council and the former Commission on Human Rights.[171] Terrorism:

- threatens the dignity and life of innocent citizens[172]
- threatens fundamental freedoms as the freedom of movement or freedom of expression as well as freedom assembly as security measures have to adapt to dangers of terrorism[173]
- has effects on the establishment of the rule of law, undermines pluralistic civil society, aims at the destruction of the democratic bases of society, and destabilizes legitimately constituted Governments[174]
- threatens the territorial integrity and security of States,[175]
- has links to serious crimes such as murder, extortion, kidnapping, hostage-taking but also to transnational organized crime, such as drug trafficking, money-laundering or illegal transfers of nuclear, chemical and biological materials[176]
- has impacts on the economic and social development of States[177].

States have an international obligation to protect persons under their jurisdiction from terrorist attacks. In the context of combating serious crimes and terrorist attacks, the ECtHR recognizes this obligation in the scope of the *right to life*, protected by Article 2 ECHR.[178] Thereby states have a positive obligation to take preventive measures to protect their citizens' lives.[179]

---

[171] See, in particular, UN Security Council, Resolution S/RES/1373 (2001), adopted on 28 September 2001, as well as Resolution S/RES/2178 (2014), adopted on 24 September 2014 and Resolution S/RES/2396 (2017), adopted on 21 December 2017; UN General Assembly Resolution A/RES/75/291 (2021); see also Human Rights Council A/HRC/14/46 (2010), Report of the Special Rapporteur Martin Scheinin.
[172] OHCHR, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet No 32 (December 2007) 7; Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 12 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[173] OHCHR, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet No 32 (December 2007) 7, 47.
[174] Daniel Byman, Terrorism and the threat to democracy, Brookings Policy Brief (February 2019) 1.
[175] UN Security Council Resolution S/RES/2178 (2014), adopted on 24 September 2014 and Resolution S/RES/2396 (2017) 1.
[176] OHCHR, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet No 32 (December 2007) 7.
[177] OHCHR, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet No 32 (December 2007) 8, 47.
[178] *Tagayeva and Others v Russia* App no 26562/07 and 6 others (ECtHR 18 September 2017) para 491; *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) paras 6-8, 63 ff, 69, 74; see also Human Rights Committee, CCPR/C/GC/36, General comment No. 36 (2018) on article 6 of the International Covenant on Civil and Political Rights, on the right to life, para 70.
[179] Article 2 ECHR: see *Tagayeva and Others v Russia* App no 26562/07 and 6 others (ECtHR 18 September 2017) para 491; in another context *Öneryildiz v Turkey* App no 48939/99 (ECtHR 30 November 2004) para 90, 101.

From the point of view of the state, the use of AI systems in the field of counter-terrorism helps to make an accurate and precise quick pre-selection, as the high amount of data[180] cannot be analysed by humans any more. Thereby, a chance can be seen in the ability of AI systems to evaluate rationally the effectiveness of surveillance models.[181] Metrics - as recall (percentage of times a model identifies an attacker) – can provide precision and accuracy.[182] If the law determines the authorized persons who get access, it reduces risks of abuse.[183] Looking at the challenges from the other side, an important question is to what extent AI tools can „*mitigate human bias in decision making*"[184] and thus to minimize discriminatory structures,[185] if data is selected not „*arbitrarily*",[186] but *carefully*[187]. Likewise, if transparency would be clearly determined[188] it might improve the effectiveness of the remedies. The suspect must know about the use of AI tools and how the algorithm works to assess its gaps[189]. These issues will be analysed in more detail below, with an examination of the relevant ECtHR case law.

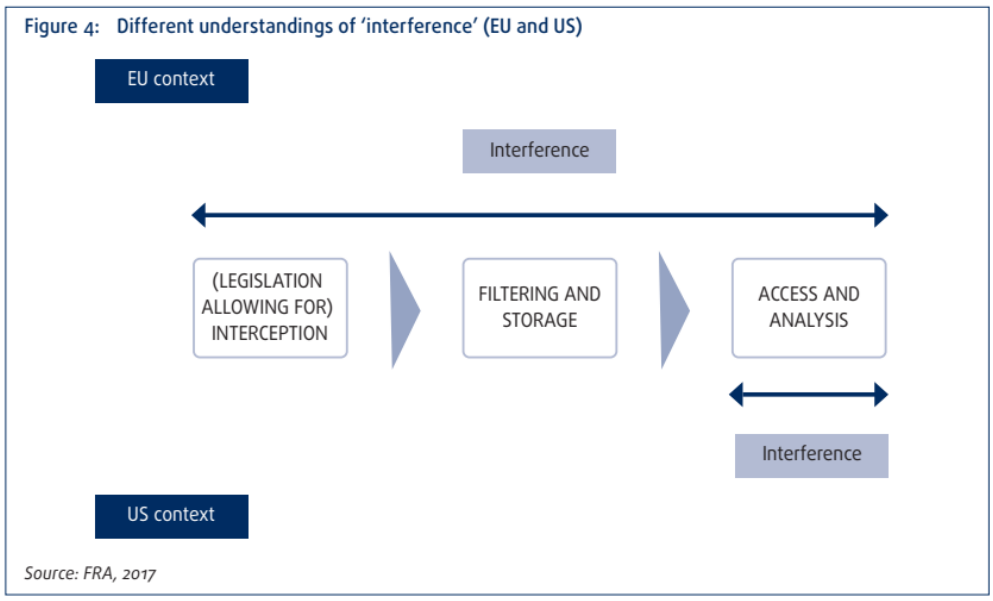
2. Right to respect for private life (Article 8 ECHR)

2.1. Overall aspects

The right to privacy is guaranteed for example in Articles 8 ECHR, 7 and 8 CFR, 11 of the American Convention on Human Rights, 12 UDHR, 17 ICCPR, 16 Convention of the Rights of the Child and Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families. The thesis will focus on the ECHR. According to a study of FRA, while in the United States an interference is not yet considered when intelligence collects data but use the data, based on European standards an interference occurs already with implanting laws on data collection and actually collecting data.[190]

---

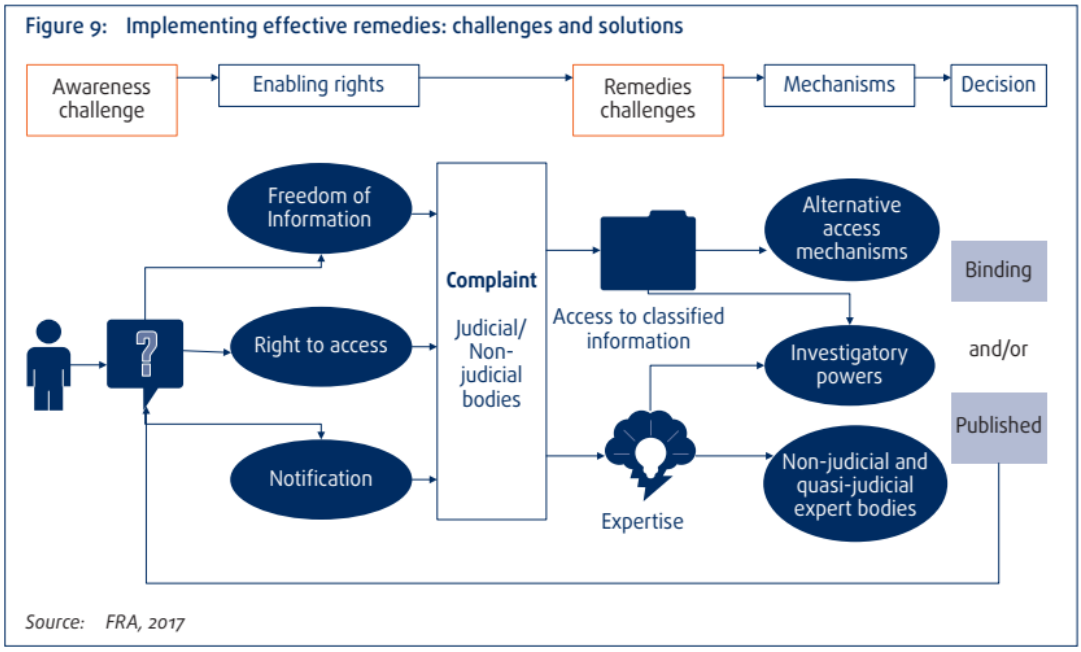
[180] Human Rights Council, UNHCR Report (A/HRC/48/31) para 13.
[181] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 26
[182] Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism (2019) 26
[183] *Weber and Saravia v Germany* App no. 54934/00 (ECtHR [GC] 29 June 2006).
[184] Report by the Islamic Military Counter Terrorism, AI and Counterterrorism (2020) 9.
[185] FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 103.
[186] United Nations General Assembly (2014), 'Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age'.
[187] Janneke Gerards, Raphaële Xenidis, Algorithmic discrimination in Europe (2020) 122.
[188] This is also one of the main critics and thus innovative rules are proposed in the Proposal for the Artificial Intelligence Act pages 7, 14, page 29, see in particular *(43): information to users and (69): transparency towards the public,* further *Article 1 lit (c), Article 13 and 52.*
[189] See Janneke Gerards, Raphaële Xenidis, Algorithmic discrimination in Europe (2020) 41.
[190] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 35.



Source: European Union Agency for Fundamental Rights[191]

The right to privacy can be violated by a variety of measures, may it be targeted or bulk surveillance, intercepting one's correspondence, collecting personal information, retaining personal or biometrical data as photographs, videos or voices,[192] i.e. basically any potential method mentioned in Chapter IV. The Court found violations of Article 8 ECHR in particular with regard to means of secret surveillance, may it be for instance in cases of interception of phone communications[193] or bulk interception of communications.[194] However, in many cases a violation was caused by the lack of safeguards to effective guarantees against arbitrariness and the risk of abuse.[195] Safeguards and remedies include notification and access to one's data as well as remedies to correct or delete data (see Article 13).[196]

[191] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 35.
[192] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 33.
[193] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015).
[194] Kennedy v The United Kingdom App no 26839/05 (ECtHR 18 May 2010); Klass and Others v Germany App no 5029/71 (ECtHR 6 September 1978); Centrum för Rättvisa v Sweden App no 35252/08 (ECtHR [GC] 25 May 2021); Big Brother Watch and Others v The United Kingdom App no 58170/13 (ECtHR [GC] 25 May 2021).
[195] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 365-374; *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021); *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 231 ff.
[196] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 113.



Source: European Union Agency for Fundamental Rights [197]

2.2.Admissibility

A specific issue in the context of AI-based counterterrorism is the question under which conditions a person can claim '*be the victim of a violation*' (Article 34 ECHR) by the application of AI technology. Relevant in the context is the case *Zakharov v. Russia*.[198] The ECtHR allowed an *in abstracto* application with regard to a violation of Article 8 ECHR because the *mere existence* of a law permitting surveillance constitutes an interference in itself. Thereby two conditions must be met: First, the applicant must be potentially affected by the scope of the law. Second, the decisive factor is whether effective remedies are available in national law. In the absence of effective remedies, the ECtHR considers the mere existence of legislation authorizing surveillance as an interference with the right to private life.

[197] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 113.
[198] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 171, 229-231; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) paras 118-129.

2.3.Scope of the right to private life

Article 8 para 1 ECHR guarantees to everyone '*the right to respect for his private and family life, his home and his correspondence*.' It is recognized that the protection of personal data is of fundamental importance to a person's enjoyment of their right guaranteed by Article 8.[199]

a) Any kind of data related to the identification of a person

The Court understands the concept of 'personal data' as '*any information relating to an identified or identifiable individual*'.[200] This means under the protection of Article 8 is information directly identifying a person such as forename and surname[201] as well as indirectly identifying a person as an IP address[202]. The common dominator is the *unique information* on the individual concerned and allowed his/her identification in a wide range of circumstances.[203]

Therefore, Article 8 protects data of various kinds, as f.i. collected by the police from an Internet provider with a dynamic identifiable IP address,[204] by surveillance cameras,[205] GPS monitoring indicating the whereabouts and movements of the subject.[206] It becomes highly sensitive, when the data might reveal a person's ethnic or origin, bearing in mind the rapid pace of developments in the field of genetics and information technology.[207] This concerns biometric data such as cellular samples,[208] fingerprints,[209] DNA profiles[210] and voice samples[211]. In the same way protected are the storage of data on someone's political affiliations of a persons or activity[212] and intimate or sensitive data revealing such as information on a person's health[213].

---

[199] Council of Europe, Guide on Article 8 of the European Convention on Human Rights (CoE 2021) para 200.
[200] *Amann v. Switzerland* App no. 27798/95 (ECHR [GC], 16 February 2000) para 65.
[201] *Garnaga v. Ukraine* App no. 20390/07 (ECtHR 16 May 2013) para 36.
[202] *Benedik v. Slovenia* App no. 62357/14 (ECtHR 24 July 2018) paras 107-109.
[203] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 85.
[204] *Benedik v. Slovenia* App no. 62357/14 (ECtHR 24 July 2018) paras 108-109.
[205] *Antović and Mirković v. Montenegro*, App no. 70838/13 (ECtHR 28 February 2018).
[206] *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010).
[207] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 71.
[208] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008); *Trajkovski and Chipovski v. North Macedonia* App nos. 53205/13 and 63320/13 (ECtHR 13 June 2020) para 40.
[209] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008); *Gaughran v. the United Kingdom* App no. 45245/15 (13 June 2020).
[210] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) paras 70- 77; *Aycaguer v. France* App no o. 8806/12 (ECtHR 22 June 2017) para 45; *Dragan Petrović v. Serbia* App no no.75229/10 (ECtHR 14 April 2020) para 69.
[211] *PP.G. and J.H. v. the United Kingdom* App no 44787/98 (ECtHR-III 25. September 2001.
[212] *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) paras 43-44; *Catt v. the United Kingdom* App no 43514/15 (ECtHR 24 January 2019) para 112, 123.
[213] *Mockutė v. Lithuania* App no. 66490/09 (ECtHR 27 February 2018) paras 93-95.

While the prior consent to the transmission or disclosure of the data is an important factor, it is, however, not decisive in determining whether a measure amounts to an interference with their right to respect for private life.[214] This becomes specially clear with regard to secret measures. They would be impossible, if the data subject would need to consent to them.

b) Public and private data

Article 8 protects public as well as private data. The fact that personal data is already (accessible by the) public does not hinder the protection.[215] Even if public, data still can be associated with the 'private life' in terms of Article 8 when collected and stored in a systematic manner,[216] which does not have to be necessarily through the means of secret surveillance.

2.4. Criteria for the Justification of the interference

Article 8 does not grant an absolute right. Restrictions are possible under the conditions of paragraph 2. Thus, to be permitted, the interference has to be '*in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.'

a) … in accordance with the law

The wording '*in accordance with the law*' requires the measure to have a basis in the domestic law and to be compatible with the rule of law. The law must be accessible to the person concerned and foreseeable as to its effects.[217] However, as the Court held f.i. in *Big Brother Watch v The United Kingdom*, the criterion of '*foreseeability'* in the context of secret surveillance cannot mean that concerned persons are able to foresee when the authorities are likely to observe them, because otherwise they may as well adapt their conduct accordingly.[218] It rather

---

[214] *M.S. v. Sweden* (Report of the Commission, 11 April 1996) para 32: There is, right to veto against the access to information contained in public documents. Furthermore, there is no right for the individual concerned to be consulted before such information is disclosed or to be notified of the disclosure afterwards.
[215] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland App no. 931/13 (ECtHR [GC] 27 June 2017) para 134.
[216] *Peck v. the United Kingdom* App no. 44647/98 (ECtHR 28 January 2003) paras 58-59.
[217] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 228; *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000-V) para 52; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 95; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 151.
[218] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 333; also *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 229; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 152.

requires the domestic law to be sufficiently clear to give citizens an adequate indication as to the conditions on which public authorities are empowered to resort to any such measures.[219] In addition, the law must indicate the scope of any discretion conferred to the authorities and the manner of its exercise with clarity to provide for adequate protection against arbitrary abuse.[220] Accordingly, in *Centrum för Rättvisa v Sweden* the Grand Chamber found that Sweden violated Art 8 based on three points:[221] 1) the absence of a clear law on the deletion of non-personal data; 2) the absence of a requirement to consider privacy interests when deciding to transmit intelligence material to third (foreign) parties; and the absence of an *ex post facto* review.

b) … pursues a legitimate aim

The measure must serve a legitimate aim in terms of Article 8 para 2: national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.[222] The most important aim with regard to terrorism is 'national security'. The Court emphasized that the protection of foreign, defence, and security policies and the identification of threats to the state are legitimate aims for using surveillance measures (*Centrum för Rättvisa v Sweden*).[223]

Thereby, the Court for instance found the storage of private and personal data in a secret police register of data with regard to the vetting of candidates pursued a legitimate aim for the purposes of Article 8, namely the protection of national security (*Leander v. Sweden*).[224] Similarly, GPS surveillance to investigate attempted murder for which a terrorist group claimed responsibility and in order to prevent future bomb attacks serves the interests of national security and public safety, the prevention of crime and protection of the rights of the victims (*Uzun v. Germany*).[225] The purpose of *prevention* of future attacks and '*identification of future*

[219] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 333; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 247; *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 229; *Huvig* v France App no 11105/84 (ECtHR 24 April 1990) para 29; *Weber and Saravia v Germany* App no 54934/00 (ECtHR [GC] 29 June 2006) para 93.
[220] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 333; *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 230.
[221] *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) paras 369-377.
[222] See also Art 11 lit a of the Data Convention 108 +.
[223] *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 279.
[224] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 49.
[225] *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) para 78. In this case the applicant was suspected of an involvement in bomb attacks and had complained that his surveillance via GPS and the use of data obtained violated his right to private life. The claim was about the data, that was collected while he was only a suspect. However, the Court found no violation of Art 8.

offenders'[226] is recognized as a legitimate aim to set up databases and collect personal information about convicted persons as well as suspects. Thereby the seriousness of the crime played a relevant role.[227] This interest may weigh even higher than the protection of biometric data, as held in *S. and Marper v. the United Kingdom* regarding fingerprint and DNA information.[228]

Specifically with regard to terrorism, the state's obligation under Article 2 – to protect the right to life of its citizens – has to be taken into consideration when looking at the legitimate aim. The authorities are obliged to take preventive measures to protect an individual whose life is at risk in the case of simple criminal acts of another individual (*Osman v The United Kingdom*).[229] This applies even more when a whole society is at risk (*Mastromatteo v Italy*),[230] especially in cases of possible terror threats.[231] In *Tagayeva and Others v Russia* the Court highlighted that the State has breached its obligation under Art 2 by taking inadequate measures, which did not prevent the terror attack.[232] The Court recognizes the retention of data of previous suspects for the purposes of the identification of future offenders in the interest of national security even in cases where the charges against the applicant had been dropped.[233] Similarly, in *Uzun v Germany* the Applicant was not convicted, but only suspected of participating in terror offences and kept under surveillance, yet the Court found no violation of Art 8.[234]

c) … is necessary in a democratic society

In order to be necessary in a democratic society, any measure interfering with the protection of personal data under Article 8 must meet a 'pressing social need'.[235] This answers in particular if the interference *'is proportionate to the legitimate aim pursued and if the reasons adduced*

---

[226] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 100.
[227] Here with regard to serious criminal sexual offences: *Gardel v France* App no 16428/05 (ECtHR, 17 March 2010) para 63; *MB v France* App no 22115/06 (ECtHR, 10 May 2010) para 54.
[228] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 104.
[229] *Osman v The United Kingdom* App no 87/1997/871/1083 (ECtHR 28 October 1998) para 115; *Edwards v The United Kingdom* App no 46477/99 (ECtHR 14 June 2002) para 54.
[230] *Mastromatteo v Italy* App no 37703/97 (ECtHR [GC] 24 October 2002) para 69; *Choreftakis and Choreftaki v Greece* App no 46846/08 (ECtHR 17 January 2012) paras 48-49.
[231] *Tagayeva and Others v Russia* App no 26562/07 and 6 others (ECtHR 18 September 2017) para 482.
[232] *Tagayeva and Others v Russia* App no 26562/07 and 6 others (ECtHR 18 September 2017) para 491.
[233] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 3, 100.
[234] *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) paras 6-8, 63 ff, 69, 74: the main reason was that the Law provided for adequate safeguards. The same applies to the present case.
[235] *Vicent Del Campo v Spain* App no 5527/13 (ECtHR 6 November 2018) para 46; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 101.

by the national authorities to justify it are "relevant and sufficient"".[236] In the Court's view, powers of secret surveillance against citizens are tolerable in so far as strictly necessary for safeguarding the democratic institutions.[237] Therefore, the measures must be applied only when necessary in a democratic society, while providing for adequate and effective safeguards against abuses (*Big Brother Watch and Others v The United Kingdom*).[238] For instance, the retention of photos taken during an investigation may be necessary also after the actual arrest of the suspect for the purposes of countering crime.[239]

The question of necessity corelates with the proportionality. In that sense, the retention of data may be necessary at first, but may become unnecessary after a certain period of time or with regard to certain parts of the data. Accordingly, the indefinite retention in a database of fingerprints, cellular samples and DNA profiles of only suspected but not convicted persons regardless of the seriousness of the offence and of their age, was found to breach Article 8.[240]

d) … is effective

The use of online communication, social media and telecommunication has increased in a way which makes it is impossible for a human investigator to collect, filter and analyse those data in a reasonable time. With regard to the fight against organised crime and terrorism, the Court acknowledged, in *Breyer v. Germany*, that modern means of telecommunications and changes in communication behaviour required that investigative tools be adapted.[241] As soon as a risk of an attack becomes known the authorities must act immediately and quickly. Therefore, the intelligence need immediate knowledge about the suspects, otherwise effective monitoring, control and prevention may become impossible. Thus, surveillance can only be effective if the authorities can collect the personal data of potential suspects (usually in secret) and analyse it with appropriate speed. In my opinion, this can nowadays only be accomplished with automated

---

[236] *Vicent Del Campo v Spain* App no 5527/13 (ECtHR 6 November 2018) para 46; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 101.
[237] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 42.
[238] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 334, *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 236; *Kennedy v The United Kingdom* App no 26839/05 para 155; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 248; *Huvig v France* App no 11105/84 (ECtHR 24 April 1990) para 29: 'there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities'.
[239] *Suprunenko v Russia* App no 8630/11 (ECtHR 19 June 2018) paras 63-65. The mere fact that a photo of a suspect is included in a database does not necessarily entail a stigma of suspicion or guilt. Even though the information stored on the police computer was personal in nature, it could not be deemed intimate or sensitive.
[240] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) paras 145-125.
[241] *Breyer v. Germany* App no. 50001/12 (ECtHR 30 January 2020) para 88.

decision-making systems. As ruled in *Marper v The United Kingdom* the fight against terrorism '*depends to a great extent on the use of modern scientific techniques of investigation and identification*'.[242] However, this does not exclude that the final decision is done by a human.

e) … is proportionate

i) Overall criteria

The proportionality criterion calls for a *balance of interests*. The State's interest in protecting national security and combating terrorism, whereby justifying the storage of personal data, should be balanced against the seriousness of the interference in the suspects' private sphere. This issue is related to the quality of the data and the accuracy of the system. The higher the false accusation rate of an AI system, the less proportionate the entire model becomes..[243]

According to an analysis of the case law of the ECtHR, this is a flexible system, whereby the proportionality may depend on several factors, such as (not exhaustively)

- the duration of the retention,
- the limitation of the use for the legitimate purposes of the retention
- the limited access of the use only for specific authorities
- the seriousness of the (alleged) offence,
- the type of the data (is it intimate? does it concern beliefs and political opinions? does it concern biometrics, such as DNA?),[244]
- the age of the suspect or offender
- and, most importantly, the existence of adequate safeguards to minimize any potential risk of abuse.

[242] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 105.
[243] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 25.
[244] See also Article 6 of Convention 108+, according to which personal data revealing racial origin, political opinions, religious or other beliefs, and information on an individual's health or sex life, or on any criminal convictions, cannot be automatically processed unless domestic law provides for appropriate safeguards. Information falling within these categories is described as "sensitive".

ii) Time limitation of retention

The *duration* of the retention as well as the *type* of data play crucial roles in the proportionality test. Data should be kept only as long as needed.[245] Thereby, the Court considers whether the data collected affect the personal enjoyment of the right to respect for private life. However, the proportionality depends also on the intrusiveness of the data concerned. As reaffirmed by the Court, sensitive personal data requires greater scrutiny.[246] For instance data collection via GPS is less intrusive than '*visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings*'[247] while on the other side, the retention of cellular samples, given their nature, is *per se* protected, even if the authorities only use a certain part of this collected information.[248] Samples and DNA profiles contain a lot of sensitive information, which enables authorities to establish genetic relationships between individuals and groups and draw conclusions about their ethnic origin. That is why in *Marper v The United Kingdom* the Court found a violation of Article 8 ECHR with regard to data containing the 'genetic make-up', namely fingerprints and DNA, which could be retained indefinitely.[249]

The *indefinite* retention together with the lack of consideration of the seriousness of the offence and the sensitive type of data (as biometrics, DNA) led to a violation in *S. Marper v UK*.[250] The Court also treated a forty-year period of retention as indefinite storage, where the Court found a violation considering that the offence was not particularly serious and, while the applicant was convicted, the domestic deletion procedure was open only for not convicted persons (*Ayçaguer v. France).*[251] Similarly, in *M.K. v France* the Court found a violation with regard to a twenty-five years retention of fingerprints of not convicted persons with insufficient procedures for deletion.[252] Even in a case with a six years retention period in a database on

---

[245] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 116 ff; *Peruzzo and Martens v. Germany* app no 7841/08 and 57900/12 (ECtHR-V 4 June 2013) para 46.
[246] *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997) para 96.
[247] *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) para 52.
[248] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 73.
[249] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) paras 103-104, 113.
[250] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 119.
[251] *Ayçaguer v. France* App no 8806/12 (ECtHR 22 june 2017) paras 42-44.
[252] *M.K v France* App no. 19522/09 (ECtHR 18 April 2013) paras 44 f.

extremism (*Catt v. UK*)[253] the Court found a violation because of the lack of safeguards. A retention of one year would not lead to a violation when the stored information is "unprocessed". The Court acknowledges the need to store raw material before it can be processed, but stresses the importance of deleting such data once it is clear that it is no longer relevant to intelligence. (*Centrum för Rättvisa v Sweden*).[254] However, because of the lack of an ex post facto review, the Court found a violation even here.[255] No violation, however, was found in *P.N. v. Germany*:[256] in this case, the data was retained for five years. This was for the purpose of identifying him as a repeat offender following the initiation of new criminal proceedings against him. In this case, an individualized verification and review was guaranteed.

iii) Considering the seriousness of the crime

Regarding the duration of the retention, the *seriousness of the offence* is also a relevant factor. In *MB v France*, the Court found the retention of personal data for thirty years proportionate related to the aim pursued, the prevention of future sexual offences.[257] Similarly, in *Marper v The United Kingdom* one decisive factor for the decision that there has been a violation was that the domestic law did not consider enough the seriousness of the crime of which the person had been suspected.[258] The more severe the (alleged) crime, the more proportionate may an interference be,[259] but the domestic law has to consider this in their criteria of the retention. Eventually, also the age has to be considered. Storage of personal data may be harmful in particular with regard to minors, given the importance of their development and integration in society.[260] This question is important insofar as the blanket and indiscriminate nature of a system, which does not distinguish between the stages of an accusation (suspicion, conviction etc.) fails to reflect a fair balance between the competing public interests and private interests.[261]

---

[253] *Catt v. the United Kingdom* App no n no. 43514/15 (ECtHR 24 January 2019) paras 120-122.
[254] *Centrum för Rättvisa v Sweden* App no 35252/08 para 146 and 147.
[255] *Centrum för Rättvisa v Sweden* App no 35252/08 para 354, 357 ff.
[256] *P.N. v. Germany*, 2020 (§§ 87-90).
[257] *MB v France* App no 22115/06 (ECtHR, 10 May 2010); *BB v France* App no 5335/06 (ECtHR, 17 March 2010); *Gardel v France* App no 16428/05 (ECtHR, 17 March 2010).
[258] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) paras 125-126.
[259] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 35.
[260] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 124.
[261] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 119.

iv) Providing for adequate safeguards

By analysing the case law, the importance of *adequate and effective safeguards* becomes clear (*Weber and Saravia v Germany; Big Brother Watch and Others v UK*).[262] The risk of abuse is inherent in systems of secret surveillance where intelligence and police have access to personal data of individuals.[263] This is all the more true in light of new technologies that make it easy for authorities to obtain large amounts of data. Such volumes of data may include information from persons who do not originally belong to the targeted category. There must be guarantees against abuse[264] before and in the process of storing data and rights to challenge the decision.

Guarantees against arbitrariness and the risk of abuse are in particular clearly determined rules of procedures as regards to the criteria and conditions for the decision of retaining data. This concerns the potentially punishable acts that may lead to a surveillance measure, as well as a definition of the persons or groups of persons to be monitored; a limit on the duration of the measure, the limitation of the use for the purpose for which they were recorded, is relevant. It concerns also clear rules on the precautions that authorities must take when transmitting data to other parties, the consultation of the persons authorised to consult the database, the limited access and disclosure of the data only to authorised persons and authorities and the circumstances in which data may or must be erased or destroyed.[265] Before the storage, an important safeguard is an institutionalised authorisation by an independent authority.[266]

After the storage, most important is the right to have the case reviewed by an independent body over the issuing body's activity and in particular a control by an independent judge to

---

[262] *Huvig v France* App no 11105/84 (ECtHR 24 April 1990) paras 29, 33-34; *Weber and Saravia v Germany* App no 54934/00 (ECtHR [GC] 29 June 2006) para 95; *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 303; *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) para 69; *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 274; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 249; further *Peruzzo and Martens v. Germany* app no 7841/08 and 57900/12 (ECtHR-V 4 June 2013) para 42.
[263] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 302-305.
[264] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 103.
[265] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 30-234; *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 498.
[266] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 233, 249, 275.

review the justification for retention.[267] Especially with regard to data, abuse is so easy. This can lead to a loss of confidence on the part of those subject to the law and thus damage democracy as a whole. A special guarantee would therefore be judicial control, as this would offer the guarantees of independence, impartiality and due process.[268] The person concerned must have the right to refute and rectify a decision on data storage and the right to request for its deletion. Besides the *judicial review*, also an *Ombudsperson*, which is independent from the executive,[269] can provide for an adequate safeguard. For instance, in *Leander v Sweden* the domestic law provided for a review of the operations authorising to collect and store in secret files information on individuals by an independent Parliamentary Ombudsman (see also under Article 13).[270]

To make use of these rights, access to information to one's data is a relevant safeguard and precondition to challenge any decision on the storage. It may be justified to wait with the notification to not jeopardize the investigation.[271] In the case of *secret surveillance* the question arises, which safeguards guarantee the lawfulness of the measure? As mentioned, the most important safeguard is the (judicial) review and supervision of measures. However, before the notification, the person concerned does not know about the measure. Hence, he or she is prevented from seeking a remedy against it. Therefore, the review should be realized without the person's intervention or even knowledge and the procedures themself have to provide for adequate and equivalent safeguards on their rights (*Roman Zakharov v. Russia* [GC] para 233).[272] Such a guarantee is, first of all, the prior authorization of a surveillance measure by a judge, which creates a preliminary judicial control of the correctness of the measure (*ibid*. para 249).

Further, as a conclusion from *Zakharov v. Russia*, can follow to guarantee the prevention of abuse by an independent *ombudsman institution*, which acts quasi on behalf of the monitored persons, who are unaware of the surveillance, and carries out regular unannounced checks. This

---

[267] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 233, 275; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 119; *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 59; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 127; *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) para 56; *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 55.

[268] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 55.

[269] With regard to the independency from the executive *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 359; *Guðmundur Andri Ástráðsson v Iceland* App no 26374/18 (ECtHR [GC] 1 December 2020) paras 152-153 and 246; *Reczkowicz v Poland* App no 43447/19 (ECtHR 22 July 2021) para 223.

[270] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 65.

[271] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 287.

[272] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 233.

would create an overarching independent and institutional control of the enforcement bodies, thereby contributing to the legitimacy of the monitoring mechanism as a whole.

According to the FRA study, the ombudsman institution plays an important role in the monitoring of surveillance measures.[273] In the context of the control of surveillance, an ombudsman institution is established at least in eleven European Member States.[274] As an impressive example can serve the concept of the Finnish Ombudsman for Intelligence Services:[275] The latter, as an independent and autonomous authority, responsibly monitors the legality of the use of intelligence collection methods and the observance of human and fundamental rights in surveillance. To this end, the ombudsman is given access to relevant information and documents and can carry out inspections in the premises of the intelligence services and enforcement authorities. He/she is also empowered to order the termination of measures based on an unlawful surveillance technique, with this order eventually being approved by the courts.[276]

In my view, this concept generally creates additional control and is particularly important in the case of secret surveillance. However, as soon as notification to the person is possible without jeopardizing the measure, the data subjects should be informed.[277] Once the data subject is informed, he or she can apply the appropriate judicial remedies themselves.

Specific consideration is given to *mass* or *bulk surveillance* in demarcation of targeted surveillance. The Court repeatedly expressed that the use of a bulk interception regime is not per se contrary to Article 8 ECHR.[278] At the same time, the Court underlines that, in light of the rapid evolution of modern communications technologies, the protections afforded by laws governing targeted surveillance must be adapted to take into account the special characteristics of bulk surveillance.[279] This is because there is a greater risk of abuse of mass surveillance and the legitimate need for secrecy in such operations. Therefore, the Court said, mass surveillance

---

[273] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 64, 65, 70, 111, 112.

[274] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 112 (year of examination: 2017).

[275] See for the following: FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 43.

[276] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 43.

[277] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 287.

[278] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) paras 322-323; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 261.

[279] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) paras 322-323; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 261.

must be subject to independent authorization at the outset, when the subject matter and scope of the operation are determined, an subsequently to independent ex post review. The measure must be evaluated for its necessity and proportionality at each stage of the process.[280]

2.5. Margin of appreciation

Eventually, Member States enjoy a wide margin of appreciation in choosing the best means to pursue the legitimate aim of protecting national security (*Big Brother Watch and Others v UK; Weber and Saravia v Germany*),[281] especially when there are adequate and effective safeguards and guarantees against abuse.[282] This assessment depends on all the circumstances of the case, such as the scope and duration of the possible measures, the degree of determination of the legal criteria for authorization, the authorities responsible for authorization, implementation and monitoring, and also, most particularly, the nature and degree of effectiveness of the legal remedy available to the persons concerned on the domestic level to challenge the measure.[283]

3. Specific aspects of the prohibition of discrimination (Article 14 ECHR in conjunction with Article 8 ECHR)

3.1. No *unreasonable* distinction based on personal characteristics

Avoiding discrimination is an effort that runs through all institutions dedicated to fighting terrorism. One of these is the OSCE which implements effective measures to countering terrorism.[284] However, '*[a]t the same time, participating States[285] unequivocally reject the association of terrorism with any particular race, nationality or religion. The organization is therefore resolute in implementing effective measures to prevent and combat terrorism, in all its forms and manifestations, as a serious crime that has no justification, whatever its motivation or*

[280] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) paras 322-323; *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021) para 261.
[281] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 338; *Weber and Saravia v Germany* App no 54934/00 (ECtHR [GC] 29 June 2006) para 106.
[282] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 339.
[283] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 339; Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 35.
[284] See https://www.osce.org/countering-terrorism (accessed 6.8.2022).
[285] To date, the OSCE has 57 participating States from Europe, Central Asia and North America, see https://www.osce.org/participating-states (accessed 6.8.2022).

origin may be. '[286] The prohibition of any discrimination is also a central provision in the ECHR. Article 14 ECHR states that the enjoyment of the rights and freedoms set forth in the Convention shall be secured without discrimination on any ground such as sex, race, colour, national or social origin or any other ground.[287] It is important to measure the issue of biases against the criteria of the ECtHR. The Court considers direct discrimination in the sense of Art 14 ECHR as a '*difference in the treatment of persons in analogous, or relevantly similar, situations*' (*Biao v Denmark*)[288] or, *a contrario sensu*, similar treatment to persons in different situations, without '*objective and reasonable justification'* (*Carson and Others v UK*).[289] Thereby the Court grants a certain margin of appreciation in assessing whether and to what extent differences in similar situations justify a different treatment.[290]

Therefore, the law may not distinguish the legal consequences based on personal characteristics of the persons concerned, such as '*sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status*' (the list is not exhaustive[291]). Nor may the algorithms per se be 'sharper' with respect to particular groupings. However, in my opinion, differentiation based on personal and individual characteristics may be reasonable and thus justified if this can be verified with high-quality data and a corresponding quantity of this data - hence measurability - whereby this verifiable and accessible. Statistics are extremely valuable information for the prevention of future attacks, and the information related to the suspects may well concern their person, for example, their political views. Thus, in my view, it would not only be justified but mandatory to classify someone who posts Nazi-glorifying slogans on Facebook as dangerous with regard to right-wing extremist acts and to train the algorithm accordingly.

---

[286] See https://www.osce.org/countering-terrorism (accessed 6.8.2022); OSCE Consolidated Framework for the Fight against Terrorism, PC.DEC/1063, Decision No. 1063, 934th Plenary Meeting (7 December 2012) Annex, 5.
[287] See also Articles 21 CFR, 14 and 26 ICCPR.
[288] *Biao v Denmark* App no 38590/10 (ECtHR [GC] 24 May 2016) para 89: 'The Court has established in its case-law that only differences in treatment based on an identifiable characteristic, or "status", are capable of amounting to discrimination within the meaning of Article 14. Moreover, (…) there must be a difference in the treatment of persons in analogous, or relevantly similar, situations (…). Article 14 lists specific grounds which constitute "status" including, *inter alia*, race, national or social origin and birth. (…)'.
[289] *Carson and others v The United Kingdom* App no 42184/05 (ECtHR [GC] 16 March 2010) para 61; *Molla Sali v Greece* App no 20452/14 (ECtHR [GC] 19 December 2018) para 135; *D.H. and Others v The Czech Republic* App no 57325/00 (ECtHR [GC] 13 November 2007) para 175 (the case also refers to indirect discrimination); *Hoogendijk v the Netherlands* App no 58641/00 (ECtHR [dec] 06 January 2005).
[290] *Fabris v France* App no 16574/08 (ECtHR [GC] 7 February 2013) para 56; *Stec and Others v The United Kingdom* App nos 65731/01 and 65900/01 (ECtHR [GC] 12 April 2006) para 51.
[291] *Biao v Denmark* App no 38590/10 (ECtHR [GC] 24 May 2016) para 89.

3.1.High quality of data to ensure unbiased systems

However, it has been suggested that automated systems supported by incorrect evidence are more likely to make incorrect decisions than humans making decisions based on the same evidence.[292] AI systems carry a risk of reproducing discriminatory patterns and thereby also reinforcing them. This may be the case when the stereotyping data influence the design of the systems; for example, when such datasets are used to train machine learning models. Finally, the decisions made based on biased AI systems can be discriminatory.[293]

As a consequence, the right to be protected from discrimination implies the obligation of state actors to ensure *high quality* of data feeding AI systems. As the systems often work with datasets, the decision will depend a lot on the quality of the collected data.[294] The data should be as inclusive as possible of all social classes, ethnicities, and population groups.[295] A crucial question is to what extent the data influence the behaviour of the system and thus its decisions in advance. If the data provided to the system is unbalanced, of poor quality, or even biased, the system could make decisions that are influenced accordingly.[296] If stereotypes and prejudices against certain population groups have already been reproduced in the dataset before these data are even processed, there is a risk of discriminatory decisions.[297] Thus, from my point of view, it is important to emphasize that the methods to prevent discrimination must be used already at the stage of data collection and not only when the algorithm or AI system is used.

One issue is '*feedback loops*': When predictive systems base their automated decisions on historical data, this implies the risk of repeating the results of previous biases and discriminatory practices. As a result, each new decision based on the system may generate new data that disproportionately suspect members of certain marginalized groups and, to that extent, bias decisions.[298] In particular, it is sensitive, when the biased data is historical criminal justice data.

---

[292] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 9 f.
[293] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 17.
[294] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 408.
[295] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 421.
[296] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 5.
[297] Österreichischer Rat für Robotik und Künstliche Intelligenz (2018) 48; Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 408.
[298] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 17; Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism, The Royal Institute of International Affairs (2019) 21.

If such historical data will be used unfiltered for the algorithm designed to prepare (intelligence or judicial) decisions, the algorithms may simply reproduce the same bias. According to the Global Terrorism Index 2022, in the years between 2007 and 2021 in total 60 per cent of fatalities from terrorism that was carried out in western states have been attributed to Islamic groups, while 30 percent have been attributed to far-right groups.[299] Such data can, of course, also influence the patterns stored in AI systems so that the system is alerted to certain groups of people. Similarly, is the issue of '*confirmation bias'*, when humans seek out evidence that confirms their hypothesis on hand.[300]

3.2.Required distinction with regard to the offence

Now, there is to distinguish between a general consolidation of discrimination patterns and specific discrimination in the individual case. The prove that the system is biased, the data for example because of inferior quality of the data sets or biased algorithms, could be difficult in view of the lack of transparency in most cases. At the same time, however, the data subject must himself claim to have been the victim of a violation of Article 14 ECHR as a result (this is an issue of admissibility, see Article 34) and in addition, he has to prove the actual affect for him in order to be entitled to compensation himself. Whether such proof is also required at the national level is left to the discretion of the individual legal systems; here, for example - as already suggested in the case of transparency - an easing of the burden of proof as for instance established with the rule of a 'prima facie evidence' could be considered.

As the retention is *discriminatory* when the domestic law does not distinguish between convicted and innocent persons,[301] this criterion is a decisive factor to implement laws in compliance with Article 8. Thus, national laws shall determine a distinction with regard to the 'stage' of accusation of the person concerned. They shall distinguish between several degrees of charges (merely suspected, trial discontinued, convicted, etc.) and express this distinction in the legal consequences. There could be undue discrimination with regard to the retention period. According to the Court's case law there has to be a distinction in the domestic law between convicted and innocent persons (not convicted), however, it may become complicated with persons who's trial has been discontinued. The Court decided for a violation of Article 8 ECHR

[299] Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 32 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).
[300] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 10.
[301] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 122.

(within the proportionality test), where the data of the data subject was '*retained indefinitely in the same way as the data of convicted persons*' (*S and Marper v The United Kingdom*).[302]

4. Specific aspects of the right to an effective remedy (Article 13 ECHR in conjunction with Article 8 ECHR)

Article 13 protects the right to an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.[303] Both control mechanisms, i.e. independent authorities overseeing surveillance activities, as well as easy and transparent access to effective remedies for the persons concerned play a relevant role here.

4.1. Data protection supervisory authority

a) The importance of establishing a specialized authority

A strong monitoring mechanism is a precondition for an intelligence accountability system. Effective oversight has the following key **elements**: (1) cooperation among key stakeholders, (2) full access to intelligence information, (3) sufficient resources, (4) transparency, and (5) independence[304] and, moreover, it was stated that an important competence is the ability to initiate investigations on their own[305] as well as the competence to stop monitoring measures and the correction or deletion.[306] An essential condition is that '*the supervisory body has access to all relevant documents, including closed materials*' (*Roman Zakharov v Russia*).[307] Looking ahead to the EU, in most Member States the judiciary and expert bodies have competences for surveillance, while parliamentary committees focus on strategic surveillance policy.[308] It is noteworthy that – only – seven EU Member States have established their own data protection authorities that also have powers over intelligence services, which is justified by the fact that international data protection rules usually exempt national security.[309]

---

[302] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 122.
[303] See also Articles 47 CFR, 14 und 3 Section 2 ICCPR.
[304] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 73.
[305] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 78.
[306] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 78.
[307] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 281; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 166.
[308] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 9.
[309] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 9.

Inspiration can be drawn from the General Data Protection Regulation (GDPR), according to which for effective compliance control, the supervisory authority has powers of investigation (access and collection of necessary information), intervention (ordering corrective measures, banning data processing, warning or admonishing the data controller, referring the matter to national parliaments and other political institutions), and engagement in legal proceedings.[310]

Whether it should be desired to have access to data '*not only that relating to specific operations, but also to internal policies and guidance*'[311] is, in my opinion, questionable if it is not relevant for the specific case. The purposes of keeping internal processes and guidelines secret must be carefully weighed against the advantages for clarifying the individual case, or procedural instruments must be used, such as the separation of proceedings or the secrecy of evidence, so that the internal intelligence processes can continue to remain secret for security reasons.

b) Independency

A national authority in terms of Article 13 can be a judicial body in the strict sense, a tribunal in terms of Article 6 para 1 ECHR[312] and a quasi-judicial body such as an administrative authority, as long as it is *independent*.[313] With regard to the 'effectiveness', the Court considers the procedural powers and guarantees implemented by the body in question.[314] A hierarchical appeal to a direct supervisor of the authority whose actions are being challenged would not be independent enough to guarantee protection against abuse.[315] Further, it is not sufficient, that the authority is by law obliged to act independent, rather its independency has to be established and function institutionally, in particular *independent from the executive*.[316] Relevant aspects

---

[310] GDPR, Art 57.
[311] As it has been suggested by FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 79.
[312] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 55, 67; *Driza v Albania* App no 33771/02 (ECtHR 13 November 2007) para 116; *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 59, 69; *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 233, 275, 292; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 119.
[313] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 65; *Segerstedt-Wiberg and Others v. Sweden,* App no 62332/00 (ECtHR 6 June 2006) para 117.
[314] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 65; *Segerstedt-Wiberg and Others v. Sweden,* App no 62332/00 (ECtHR 6 June 2006) para 117.
[315] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 299.
[316] *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021) para 359; *Guðmundur Andri Ástráðsson v Iceland* App no 26374/18 (ECtHR [GC] 1 December 2020) paras 152-153 and 246; *Dolińska-Ficek and Ozimek v Poland* App nos 49868/19 and 57511/19 (ECtHR 8 November 2021) para 279; *Reczkowicz v Poland* App no 43447/19 (ECtHR 22 July 2021) para 223.

are the manner of appointment of its members, their duration term of office, guarantees against outside pressures and their appearance of independence.

Thus, oversight bodies must themselves be subject to *public scrutiny* and have the capabilities to be held accountable.[317] Thereby the ECtHR underlines that control should be established in form of a liability capable of redressing individual grievances caused by secret surveillance or to control effectively the functioning of the surveillance bodies.[318]

The authority should be as transparent as possible. This could be achieved by providing public reports and information about their activities. Due to their independent status, the Council of Europe Commissioner for Human Rights deems them as being ideally placed to provide reliable information to make the public aware about the role of intelligence services.[319] Complete transparency is, of course, not possible due to the nature of secret surveillance.[320]

In line with the ECtHR case law and according to UN standards, oversight mechanisms shall be independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary, capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.[321] Not entirely in line with the UN standards and the ECtHR case law, the FRA study shows that some oversight bodies are heavily dependent on the executive bodies.[322] However, to my opinion, with regard to the executive, one has to distinguish two issues. While, on the one hand, the involvement of governmental departments concerned (e.g. Chancellery, Foreign, Interior or Defence Ministry) contributes to the effectiveness of intelligence services' accountability systems control by the executive is, on the other hand, not considered as sufficiently independent.[323] This has to be considered when creating an effective accountability system.

---

[317] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 12, 56.
[318] *Szabo and Vissy v. Hungary* App no 37138/14 (ECtHR 12 January 2016) para 82.
[319] Council of Europe Commissioner for Human Rights (2015), p. 65; FRA 87.
[320] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 87.
[321] UN General Assembly, A/RES/71/199 (January 2017), Resolution adopted by the General Assembly on 19 December 2016, The right to privacy in the digital age, para. 5(d).
[322] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 11: For instance, the law does not grant them binding decision-making powers, they have limited staff and budgets, or their offices are located in government buildings.
[323] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 60.

c) The power to issue binding decisions

The competence to issue binding decisions is a key element of an effective remedy. At a minimum, this should include the right to order the termination of the monitoring, to obtain the destruction of the stored data and to award the data subject appropriate compensation.[324]

4.2.Effective remedy

a) In general

A frequent criticism is that remedies against data surveillance do not exist or are not known to those subject to legal protection, while a notification that one is subject to secret surveillance is a necessary prerequisite.[325] Exactly the lack of an effective remedy often leads to a human rights violation; that was the case for example in *Rotaru v. Romania*[326] because the applicant did not have a remedy to challenge the storage of data concerning his private life or the veracity of that information; also in *Segerstedt-Wiberg and Others v. Sweden*[327] because the applicants could not view the entire information about them in the security police files and obtain their destruction, neither could they let delete or rectify the personal information in those files; similarly in *Nada v. Switzerland*,[328] because the applicant did not have a remedy to request the deletion of his name from the list annexed to the Taliban Ordinance. Therefore, the criteria of an effective remedy in terms of Article 13 ECHR will be examined in more detail below.

b) Effectiveness in terms of Article 13 ECHR

The remedy must be accessible and capable of directly remedying the merits of the case (*Hasan and Chaush v Bulgaria*).[329] In the context of secret surveillance, the Court held in *Klass and Others v Germany* that a remedy has to be as effective as it can be having regard the restricted scope for recourse inherent in the context of surveillance for the purposes of preventing crimes, as in the context of terrorism.[330]

As a notification could jeopardize the secret surveillance, it is not a mandatory requirement.[331] However, after notification of the measures, the person concerned must be provided

---

[324] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 114.
[325] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 10.
[326] *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 67- 73.
[327] *Segerstedt-Wiberg and Others v. Sweden*, App no 62332/00 (ECtHR 6 June 2006) paras 116-122.
[328] *Nada v. Switzerland* App no 10593/08) (ECtHR [GC], 12 September 2012) paras 209-214, in particular 213.
[329] *Hasan and Chaush v Bulgaria* App no 30985/96 (ECtHR [GC] 26 October 2000) para 100.
[330] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 78-79.
[331] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 58 and 71; *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 66, 78-84.

with legal remedies within a reasonable period of time.[332] Such remedies could bring the rights to get *access* to the data as well as *rectify* and *delete* the stored data; further, the right to let the decision be *reviewed* by an independent body as to whether the surveillance measures complied with the law. As mentioned under Article 8 (VII.2.4.e)iv), the reviewing instance shall be independent and impartial, which may be a judicial body,[333] but can be also an Ombudsperson (as f.i. in *Leander v Sweden*: independent Parliamentary Ombudsman).[334]Moreover, they could contain the right to claim for *compensation* of damages before a civil court.[335] However, one must consider the whole system as the Court consistently emphasizes that even where no single remedy may itself entirely satisfy the requirements of Article 13, the aggregate of remedies provided for under domestic law may meet them (*Leander v Sweden; Chahal v The UK*).[336]

c) The (Non)-Transparency as an issue of an effective remedy

In general, in cases concerning the storage of personal data, Member States have to ensure that the persons concerned get access to all the information related. However, with regard to secret surveillance the requirement to be transparent will be less strict as the disclosure may be too sensitive for national security.[337] To be effective, the measures must be kept secret, so it is only after the measures have been revealed, that the person concerned has to get access to legal remedies within a reasonable time (*Rotaru v Romania*).[338] However, at the same time the domestic law must offer a remedy to view the information about the applicant.

Problems with regard to the lack of transparency can occur in many ways. In particular, it may be unclear which parameters the system uses for decision making and / or which

---

[332] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) paras 287; *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 69.
[333] *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015) para 233, 275; *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 119; *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 59; *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 127; *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010) para 56; *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 55.
[334] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 65.
[335] *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978) para 71; *Nada v. Switzerland* App no 10593/08) (ECtHR [GC], 12 September 2012) paras 209-214); *Segerstedt-Wiberg and Others v. Sweden*, App no 62332/00 (ECtHR 6 June 2006) paras 117-122.
[336] *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987) para 77 (c); *Chahal v The United Kingdom* App no 22414/93 (ECtHR 15 November 1996) para 145; *Kudła v Poland* App no 30210/96 (ECtHR [GC] 26 October 2000) para 157.
[337] *Segerstedt-Wiberg and Others v. Sweden*, App no 62332/00 (ECtHR 6 June 2006) para 102.
[338] *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000) para 69.

weighting the system uses for individual parameters to get to that specific decision.[339] The term 'black box' refers to this issue as it is difficult or impossible to trace back and explain the decision making process.[340] The issue of transparency becomes particularly tricky when the decisions are not made or even controlled by humans, but generated purely artificially.[341]

5. Specific aspects of the right to a fair trial (Article 6 ECHR)

5.1. Article 6 para 1 ECHR

a) Applicability

For the understanding of 'civil rights and obligations' the concerned domestic law as well as the autonomous concept deriving from the European Convention of Human Rights have to be taken into consideration.[342] Article 6 para 1 applies independent of the nature of the legislation governing the dispute (administrative law, civil, commercial etc.) and the nature of the domestic authority in the matter (court, administrative body etc.).[343] The civil and criminal aspects of Article 6 don't have to exclude each other, but rather may be assessed under both heads.[344] Further, the applicability of Article 6 para 1 ECHR depends on the existence of a serious and genuine dispute related to a civil right which is directly decisive for the civil right under discussion (*Károly Nagy v Hungary*; *Denisov v Ukraine*).[345] Accordingly, Article 6 (civil limb)

---

[339] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 5; Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 408; Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 11.

[340] AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019) 5; Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism 17; Janneke Gerards, Raphaële Xenidis, Algorithmic discrimination in Europe (2020) 10; Human Rights Council, UNHCR Report (A/HRC/48/31) para 20, 56; FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 35; Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 84; Andrés Páez, ‚Negligent Algorithmic Discrimination', in Law and Contemporary Problems Vol. 84:19 (2021), 24, 27; Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 9.

[341] Verónica Dahl in Emilia Gómez (ed.) 'Assessing the impact of machine intelligence on human behaviour: an interdisciplinary endeavour' (2018), 31; Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 409; Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 9.

[342] *Georgiadis v. Greece*, no. 21522/93 (29 May 1997) para 34.

[343] *Bochan v. Ukraine* (no. 2) App no 22251/08 (ECtHR [GC], 5 February 2015) para 43.

[344] Ramos Nunes de Carvalho e Sá v. Portugal App nos. 55391/13, 57728/13 and 74041/13 ([GC], 6 November 2018) para 121: 'the two aspects, civil and criminal, of Article 6 of the Convention are not necessarily mutually exclusive'.

[345] *Károly Nagy v Hungary* App no 56665/09 (ECtHR [GC] 14 September 2017) para 60; *Denisov v Ukraine* App no 76639/11 (ECtHR [GC] 25 September 2018] para 44; *Regner v The Czech Republic* App no 35289/11 (ECtHR [GC] 19 September 2017) para 99; *Lupeni Greek Catholic Parish and others v Romania* App no 76943/11 (ECtHR [GC] 29 November 2016) para 71; *Naït-Liman v Switzerland* App no 51357/07 (ECtHR [GC] 15 March 2018) para 106.

was applied to proceedings concerning the *deletion of information from databases*.[346] The reason therefore is that the inclusion of personal data in a database may affect the *reputation and private life*, and thus, for example, job prospects of the persons concerned.[347]

b) Public hearing

Issues related to the specific topic could be the lack of a *public hearing*, especially when the decision to collect and store data is merely based on an automated decision by an algorithm or an AI system and the domestic law does not provide for a judicial review. Under special circumstances, under Article 6 § 1 national security might justify the exclusion of the public from the proceedings.[348] However, in the case *Vasilev v Bulgaria*,[349] the exclusion of the public from all hearings and the delivery of the judgment had been based solely on the presence of classified information in the file (evidence from covert interception of the applicant's telephone conversation). In the Court's view, the total lack of public access could not be justified by the need to protect the classified information. Techniques exist to allow some degree of public access while at the same time maintaining the confidentiality of sensitive information.[350]

c) Justification and reasons

Article 6 para 1 obliges the courts to give sufficient reasons for their decision, which shows that the parties had their arguments heard and enables them to properly exercise the right to appeal (*Hirvisaari v Finland; Suominen v Finland*).[351]As stated by the Grand Chamber in *Denisov v Ukraine*, after verifying that a court did not comply with the requirements of an independent and impartial tribunal, which includes giving reasons to its decisions, the Court must determine

---

[346] *Užukauskas v. Lithuania* App no 16965/04 (ECtHR 6 July 2010) paras 34-39; *Pocius v. Lithuania* App no 35601/04 (ECtHR 6 July 2010) paras 38-46: The applicants were listed in a database containing information on persons deemed to be a danger to society. In administrative proceedings, they had requested the removal of their names from the database.

[347] *Užukauskas v. Lithuania* App no 16965/04 (ECtHR 6 July 2010) paras 34-39; *Pocius v. Lithuania* App no 35601/04 (ECtHR 6 July 2010) paras 38-46.

[348] *Kennedy v. the United Kingdom* App no 26839/05 (ECtHR 18 May 2010) para 188.

[349] *Vasilev v. Bulgaria* App no 7610/15 (ECtHR 16 November 2021) paras 106-111. The term 'classified information' is usually used for material containing sensitive information which should be protected.

[350] *Vasilev v. Bulgaria* App no 7610/15 (ECtHR 16 November 2021) paras 106, 116-118.

[351] *Hirvisaari v Finland* App no 49684/99 (ECtHR 27 September 2001) para 30; *Suominen v Finland* App no 37801/97 (ECtHR 1 July 2003) paras 36-37; *García Ruiz v Spain* App no 30544/96 (ECtHR 21 January 1999) para 26.

whether the review of the case was sufficient to remedy the shortcoming identified.[352] The lack of reasoning can be cured by a judicial review providing for sufficient reasons (see next point).

d) Judicial Review

However, the lack of a public hearing can be remedied by providing for a public hearing at the stage of appeal, if the Court of Appeal has full jurisdiction to review the merits of the case.[353] The same applies to the lack of reasoning. Therefore, even if the first-instance decision violates Article 6 procedural safeguards, a potential violation can be remedied if such a decision is subjected to control by a judicial organ with full jurisdiction ensuring the procedural guarantees of Article 6 para 1 (*Oleksandr Volkov v Ukraine; Tsfayo v The United Kingdom; Albert and Le Compte v Belgium*).[354] In considering the decision of the inclusion in a database, the court shall take into account several factors, such as the subject matter of the decision appealed from, the manner in which that decision was rendered, and the substance of the dispute, including the grounds of appeal (*Bryan v The United Kingdom*; *Tsfayo v The United Kingdom*).[355]

As the decisions to collect and restore data as well as the decisions against a request for a deletion will often be issued by specific administrative authorities, also the question arises, if that is sufficient for Article 6. However, even if the first instance was not a judicial body, the guarantees of Article 6 may be fulfilled if the decision by that authority is subject to subsequent review by a judicial body that has full jurisdiction and provides the guarantees of Article 6 para 1. This applies when a court of full jurisdiction remedies procedural or even structural deficiencies identified in the proceedings before the administrative body in the course of subsequent judicial review (*Ramos Nunes de Carvalho e Sá v Portugal*).[356]

---

[352] *Denisov v Ukraine* App no 76639/11 (ECtHR [GC] 25 September 2018] para 67; *Le Compte Van Leuven and De Meyere v Belgium* App nos 6878/75 and 7238/75 (ECtHR 23 June 1981) paras 51 and 54; *Oleksandr Volkov v Ukraine* App no 21722/11 (ECtHR 9 January 2013) paras 108 and 123.

[353] *Ramos Nunes de Carvalho e Sá v Portugal* App nos 55391/13, 57728/13 and 74041/13 (ECtHR [GC] 6 November 2018) para 192; *Le Compte Van Leuven and De Meyere v Belgium* App nos 6878/75 and 7238/75 (ECtHR 23 June 1981) para 60; *Albert and Le Compte v Belgium* App nos 7299/75 and 7496/76 (ECtHR 10 February 1983) para 36.

[354] *Oleksandr Volkov v Ukraine* App no 21722/11 (ECtHR 9 January 2013) para 123; *Tsfayo v The United Kingdom* App no 60860/00 (ECtHR 14 November 2006) para 42; *Albert and Le Compte v Belgium* App nos 7299/75 and 7496/76 (ECtHR 10 February 1983) para 29.

[355] *Bryan v The United Kingdom* App no 19178/91 (ECtHR 22 November 1995) para 45; *Tsfayo v The United Kingdom* App no 60860/00 (ECtHR 14 November 2006) para 43.

[356] *Ramos Nunes de Carvalho e Sá v Portugal* App nos 55391/13, 57728/13 and 74041/13 (ECtHR [GC] 6 November 2018) para 132.

5.2.Article 6 para 2 ECHR

Article 6 para 2 protects the presumption of innocence. It can be both part of the civil and the criminal limb, but is necessarily an issue in criminal proceedings. The provision stipulates, inter alia, that the judge may not assume that the suspect committed the crime with which he is charged, but shifts the burden of proof to the prosecutor, with the consequence that any doubt will benefit the defendant.[357] Of course, when data is included in databases, the potential risk of stigmatization is high. Human rights organizations rate this risk all the higher the less 'human' control behind the decisions and the more they are based on algorithms (but see VIII. on the potential benefits of AI). For databases, the Court has already pronounced that the retention of individuals' private data cannot be equated with suspicion.[358] However, in order to avoid giving the impression to the outside world that they are automatically treated as suspects, the law must take precautions to distinguish between certain groups of people. For example, data on mere suspects may not be stored for the same period of time as data on convicted persons.[359]

6. Specific aspects of the right to life (Article 2 ECHR)

According to Article 2 ECHR everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law. [360] With regard to the protection of the right to life and the relationship to the use of Artificial Intelligence, of course, any (automated) decision has to be considered the more careful the more intrusive the interference is. Article 2 ECHR prohibits targeted or extrajudicial killings of suspected or actual terrorists outside of armed conflicts.[361] In principle, '*under IHRL the intentional, premeditated killing of an individual would be unlawful, unless it is a means of last resort and strictly necessary to protect against an imminent threat to life*.'.[362] This may be the case, for instance, where there is a limited time to react to be balanced against an immense negative consequence on the protection of

---

[357] *Barberà, Messegué and Jabardo v. Spain* App no. 10590/83 (ECtHR 6 December 1988) para 77.
[358] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 122.
[359] *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008) para 122.
[360] See also Articles 2 CFR and 6 ICCPR.
[361] HRCttee, CCPR/C/GC/36 (2018) General comment No. 36 on Article 6 of the International Covenant on Civil and Political Rights, on the right to life, para 12: In times of peace, '[t]he intentional taking of life by any means is permissible only if it is strictly necessary in order to protect life from an imminent threat'.
[362] Human Rights Council, 44th session, A/HRC/44/38, Extrajudicial, summary or arbitrary executions Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions (29 June 2020) para 35; see also Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 9.

the citizens. However, even in that cases, the decision must be based on sufficient evidence and information,[363] which is why, to my opinion, it should not be based only on an automated decision of an AI system but on a human decision authorizing the act.

7. Specific aspects of the prohibition of torture (Article 3 ECHR)

An aspect of the respect for human dignity is the prohibition of torture and inhuman or degrading treatment or punishment, guaranteed in Article 3 ECHR.[364] Especially after the 9/11 attacks, critical interrogation techniques were increasingly used, bordering on torture or at least constituting inhumane or degrading treatment.[365] The scrutiny is even higher when dealing with information received from law enforcement agencies in states being famous fort their ill-treatment of suspects.[366] Often information is obtained as a result of ill-treatment or torture.[367] In this respect, on the one hand, special caution must be given when the data on which the application of an interrogation measure is based is based on automated AI decision-making processes. Further, in my view, when information is used, and then used for a database or algorithm, it would need to be disclosed that it is obtained in the course of critical interrogation activities.

8. Specific aspects of the right to liberty (Article 5 ECHR)

Article 5 ECHR secures the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law:[368] Deprivation of liberty and security of persons are principal means for impairing the enjoyment of other rights.[369] Its main aspect is the prohibition of arbitrary arrests or detention.[370] Terrorism suspects must be enabled to have access to information about the reasons for their arrest.[371]

For the application of Article 5, the arrest must take place in the context of a criminal proceeding (investigation) and under a reasonable suspicion of the suspect having committed

---

[363] *McCann and others v The United Kingdom* App no 18984/91 (ECtHR 28 September 1995).
[364] See also Articles 1 and 4 CFR, 7 and 10 ICCPR.
[365] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 12.
[366] OSCE/ODIHR, 'Human Rights In Counter-Terrorism Investigation' (2013) 28.
[367] OSCE/ODIHR, 'Human Rights In Counter-Terrorism Investigation' (2013) 28.
[368] See also Articles 6 CFR and 9 ICCPR.
[369] Human Rights Committee, CCPR/C/GC/35 (2014), General Comment Nr 35, para 2 (with regard to Article 9 of the ICCPR).
[370] Human Rights in Counter-Terrorism Investigation 71; see also (with regard to Article 9 ICCP) Human Rights Committee, CCPR/C/GC/35 (2014), General Comment Nr 35, para 11 f.
[371] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 17; Human Rights in Counter-Terrorism Investigation 71 f.

an offence (*Jėčius v Lithuania*; *Schwabe and MG v Germany*).[372] According to the ECtHR's case law, '*reasonable suspicion'* is to be applied as the threshold of proof and is an important safeguard for the suspect (*Selahattin Demirtaş v Turkey*).[373] The relevant question is whether an objective observer would be observer would be convinced that the suspect might have committed the offence in question. In the context of terrorism, on the one hand, the Court acknowledges, that States cannot be required to establish the criteria of the reasonableness of the suspicion by disclosing confidential sources of information. On the other hand, the purpose of combating terrorist offenses cannot justify extending the meaning of "reasonableness" to such an extent that the protection afforded by Article 5 § 1 (c) is compromised.

It becomes problematic when a suspicion and an arrest based on it turn out to be wrong, but the decision was made on the basis of an AI system. One of the many safeguards and rights during an arrest[374] is the right to challenge the lawfulness of one's arrest. However, that may become impossible, if and insofar the details of the algorithm or AI system which produced the decision for the arrest are not revealed to the suspect. So to my opinion the suspect and his legal support must get access to all the information necessary to create a successful appeal. However, it could be the case that the disclosure of the basis for the decision would entail a danger, the prevention of which would outweigh the preservation of the suspect's rights of defence (e.g. there is reasonable suspicion that a terrorist attack is being planned and further accomplices of the suspect could carry it out and disclosure of the basis for the decision could block the investigation). Also, in the anti-terrorism context, the police may be obliged to act with utmost urgency, often following up on information from secret sources which cannot be revealed.[375] In this case, however, the justification for the closure shall be disclosed to the suspect.

In the case of *Akgün v. Turkey*[376], at the time of the applicant's pre-trial detention, the only evidence to establish suspicion (of Article 5(1) lit c) was that he had used the ByLock encrypted messaging system. On that basis, the authorities suspected him of belonging to a terrorist organization. The Court recognized that the use of electronic evidence indicating that a person

---

[372] *Jėčius v Lithuania* App no 34578/97 (ECtHR 31 July 2000) para 50; *Schwabe and MG v Germany* App nos 8080/08 and 8577/08 (ECtHR 1 March 2012) para 72; *Selahattin Demirtaş v Turkey (No 2)* App no 14305/17 (ECtHR [GC] 22 December 2020) para 314; *Şahin Alpay v Turkey* App no 16538/17 (ECtHR 20 June 2018) para 103; *Kurt v Austria* App no 62903/15 (ECtHR [GC] 15 June 2021) para 187.

[373] *Selahattin Demirtaş v Turkey (No 2)* App no 14305/17 (ECtHR [GC] 22 December 2020) para 314. See also *Şahin Alpay* v Turkey App no 16538/17 (ECtHR 20 June 2018) para 103; *Włoch v Poland* App no 27785/95 (ECtHR 17 January 2011) para 108; *Mehmet Hasan Altan v Turkey* App no 13237/17 (ECtHR 10 September 2018) para 124.

[374] See for an overview Human Rights in Counter-Terrorism Investigation 84.

[375] Human Rights in Counter-Terrorism Investigation 88.

[376] *Akgün v. Turkey* App no 19699/18 (ECtHR 20 July 2021) summary with reference to paras 178-181.

had used an encrypted messaging service specifically designed for a criminal organization could be an important instrument in combatting organized crime. Consequently, it may also lead to the arrest of a suspect. However, if such evidence formed the sole basis for suspicion against a person, the national court was required to have sufficient information about the material in question before examining its possible probative value. In the *Akgün v. Turkey*, the government was unable to show that, at the time the pretrial detention, the evidence met the required standard of "reasonable suspicion." In the Court's view, the document concluding that suspect had used ByLock did not specify or set forth any unlawful activity on his part, as it did not specify the dates of that alleged activity or its frequency, and did not provide any further details.

On the other hand, it follows that an algorithm-based decision need not be excluded per se as evidence of pre-detention. On the contrary: based on the algorithm, a risk analysis can be made that confirms or refutes the merits of a preliminary detention. In the same way, the algorithm or the AI system could have been used, for example, to analyse postings of certain individuals on social media for their riskiness, and thus the AI system would perform the same function that a human investigator performs, but this task is hardly manageable nowadays due to the amount of data. From my point of view, the decision of the algorithm is then to be classified as 'evidence', which is ultimately subject to the final decision of the competent national authority. The key point is that the decision-making is comprehensible, explainable and accessible for the suspect, so that the suspect is also be in the factual and legal position to challenge the findings.

9. Specific aspects of the freedom of thought and connected rights

Article 9 (Freedom of thought, conscience and religion), Article 10 (Freedom of expression) and Article 11 (Freedom of assembly and association) are relative rights.[377] They may be subject to restrictions according to their paragraph 2. Interferences by the potential of AI-enabled technologies can vary. For one, AI systems can be used to influence individuals' thoughts.[378] The use of automated applications by monitoring user-generated online content, as for instance postings on social media platforms, can trigger actions based on an individual's online behaviour. In the same way, intelligence and counterterrorism agencies are using AI-enabled technologies to direct users at risk of radicalization to counter-terrorism content. This can interfere

[377] These rights are also guaranteed by other legal frameworks such as Articles 10-12 CFR and 18-22 ICCPR.
[378] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 38; Susie Allegre. 'Rethinking Freedom of Thought for the 21st century', European Human Rights Law Review, 3 (2017) 224.

with the right to freedom of thought because the interaction manipulates their thoughts. However, such an approach would be justified, in my view,[379] if "free" radicalization would otherwise amount to threats to national security. When used accurately, predictive AI systems give an opportunity for counterterrorism and early detection of radicalization (see #).

VIII. Chances for Human Rights

Despite potential dangers, one must consider also the advantages of using algorithms and AI. The large amount of data and their increasingly complex information cannot be interpreted by human intelligence alone any more.[380] Therefore, AI systems support and complement human work through cognitive interpretation and processing of data sets, bringing efficiency and remediation to decision-making processes.[381] As the use of AI creates resources and improves the accuracy of pre-selection, it also contributes to a clearer decision on whether an interference with the privacy of the data subject or other of his or her rights is justified.[382]

1. *Resource Savings*: Coping with large amounts of data

The smaller the number of profiles that intelligence analyses for patterns, the less meaningful the analyses. This is the great opportunity of algorithms and AI systems. They can collect immense amounts of data at an indescribable speed, filter this data according to specific criteria and analyse it to create a pre-decision. For instance, a study group collected automatically '*3.1 million Arabic [Twitter] tweets mentioning ISIS in some form, authored by more than 250k users between Oct. 13, 2014 and Dec. 31, 2014*' to analyse historic timelines of users supporting or opposing ISIS.[383] Machine learning models which can collect such large amounts of data are

[379] Contrary to my opinion, the # deems such an interference as unjustified: United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 38.
[380] Damien Van Puyvelde et al., 'Beyond the Buzzword: big data and national security decision-making' (2017) 1398.
[381] Emilia Gómez (ed.) 'Assessing the impact of machine intelligence on human behaviour: an interdisciplinary endeavour' (2018), 7.
[382] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 26.
[383] Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015), https://arxiv.org/pdf/1503.02401.pdf (accessed 27.7.2022).

in particular useful for classifying and learning about groupings.[384] In this way, resources can be used in a targeted manner and the quality of investigative work can be improved.

2. *Deeper Insights*: Revealing patterns and characteristics of terrorists

Exactly because of their ability to analyse large amounts of data, automated systems are more capable than human investigators to detect patterns of terrorist groups.[385] They can systematically collected data about several groups and organizations, filter the data according to certain criteria and reveal patterns or information about the group behaviour and developments. For instance, researchers have applied AI including Social-Network-Analysis ('SNA') algorithms to '*better understand the roots of this organization [ISIS] and its supporters*'.[386] It has been used also to predict fragmentations of terrorist groups by getting deeper insights on how and under why terrorist groups such as ISIL and Al-Qaida split.[387] By analysing and classifying supporters of terrorists group so far, the system can help to predict who would be likely to support the same groups in the future (see the study regarding ISIS).[388]

At the same time, AI systems and algorithms can reveal characteristics of lone-wolf terrorists who act independently, but usually connect with other sympathizers. The system can find similarities, differences and correlations to the social environment. It can even analyse which (counter-)strategies influence the terrorists' behaviour.[389] Thus, AI systems contribute to the early detection of terrorist group patterns as well as lone-wolf terrorist characteristics.

In my opinion, with this ability, citizens are better protected against terror acts, while at the same time fewer innocent citizens are suspected on the basis of false analyses (and, for example, are not admitted to a flight). Moreover, as the knowledge about terrorist profiles and behaviour sharpens the profiling system, at the same time the system will improve its accuracy

---

.[384] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 17.
[385] See for instance Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015).
[386] Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015).
[387] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 25.
[388] Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015).
[389] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 25.

when creating pre-decisions about potential suspects and will improve the success rate to the point that the classification as a terror suspect actually corresponds to the real facts.

3. *Predictability*: Increase success in preventing terrorist attacks

AI systems may be able to make better predictions in terms of group behaviours as much as lone-wolf terrorists. These systems are particularly applicable to online communication and social media.[390] Since terrorist networks and communities that share extremist fantasies communicate largely online, AI systems can analyse these communication channels and make various deductions from them.[391] They can detect levels of radicalization (see below), anticipate the emergence of new movements, and predict acute threats such as attacks.[392] AI-powered systems interpret daily online interactions and rate risk on a scale so that law enforcement or security services can prevent a thought from being put into action.[393] The system can act on a high speed and give – accurate – alerts to the competent authorities.[394]

The UN Office of Counterterrorism refers to *INSIKT* Intelligence's program as a positive example of how predictive analytics can provide deep insights into the network structure of terrorist groups and serve to reduce attacks.[395] This is a start-up company that uses machine learning models, through NLP and SNA techniques, to detect potential threats on the Internet. Used quite freely available content and data, especially on social media. The insights gained are used to detect dangerous content and threats while identifying patterns.

In my opinion, it is valuable how the system improves itself with each insight. Through the results from the data sources, the predictive models become more accurate and sharper. Of

---

[390] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 18 f; see the study of Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015); F. Johnson, M. Zheng, Y. Vorbyevaa, A. Gabriel, H.Qi, N. Velasquez, P. Manrique, D. Johnson, E. Restrepo, C. Song, S. Wuchty, 'New online ecology of adversarial aggregates: ISIS and beyond', Science 352(6292), (published 17.6.2016, http://science.sciencemag.org/content/352/6292/1459 (accessed 27.7.2022).
[391] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 18 f.
[392] N. F. Johnson, M. Zheng, Y. Vorbyevaa, A. Gabriel, H.Qi, N. Velasquez, P. Manrique, D. Johnson, E. Restrepo, C. Song, S. Wuchty, 'New online ecology of adversarial aggregates: ISIS and beyond', Science 352(6292).
[393] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 38.
[394] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24.
[395] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24; see https://www.insiktintelligence.com (accessed 26.7.2022).

course, this assumes that the data is not of poor quality or biased, because otherwise the system would also become biased. However, this is avoidable through qualitative data processing.

4. *Deradicalization*: Early detection of individuals easily seducible to radicalization

A fascinating area of use for AI systems is their aiding in the deradicalization of individuals. Effective AI systems for predicting potential threats can also be used to identify individuals vulnerable to radicalization at an early stage and help them - obviously or secretly - to deradicalize.[396] Nowadays it became impossible to detect such persons through traditional methods. Machine learning techniques such as *Natural language processing* (NLP), a tool to make machines understand language the same way as humans do (see III.1.5.) can, for instance, identify keywords indication state of radicalization of a social media account or the vulnerability of someone to extremist narratives online.[397] They can also detect patterns of behaviour related to radicalization. Some tools even detect suicide risk or vulnerability to mental health problems, and as they evolve, they can also assess vulnerability to violent extremist ideologies.[398] On the European level, the project '*Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing*' (short: RED-Alert) aims to detect early stages of radicalization while at the same time trying to ensure protection of privacy and security.[399] It does so by developing '*natural language processing (NLP), semantic media analysis (SMA), social network analysis (SNA), Complex Event Processing (CEP) and artificial intelligence (AI) technologies.*'[400] Something specific about this tool is its ability to anonymize and de-anonymize data, which is in particular important when dealing with sensitive data.[401]

One of the most promising projects is the '*Redirect Method*', a program developed by the private company Jigsaw, a subsidiary of Alphabet Inc. It aims to detect vulnerable persons

---

[396] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 5; United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24.
[397] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24.
[398] Jigsaw (2016). 'The Redirect Method', www.redirectmethod.org (accessed 19.7.2022).
[399] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 26. The project is supported by Europol and specific activities around the World Counter-Terrorism Summit: https://cordis.europa.eu/project/id/740688/de (accessed 26.7.2022).
[400] RED-Alert Homepage: https://cordis.europa.eu/project/id/740688/de (accessed 26.7.2022).
[401] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 26.

before being seduced by extremist ideologies. The *Redirect Method* is an '*open-source methodology that uses targeted advertising to connect people searching online for harmful content with constructive alternative messages*.'[402] Thereby, for instance, it targets online users of video-sharing websites who may be attracted to the propaganda of terrorist networks such as Islamic State of Iraq and Syria (ISIS), and *redirects* them to other videos which can provide for a credible counter-narrative.[403] Thus, they will be connected to "positive messages".[404]

Thus, trustworthy systems can help to intervene early and stop young people from being seduced by extremist ideologies in the world.[405] Further, precisely they can ensure the necessary unequal treatment between actual assassins and those merely inclined to radicalization (Article 14), and preserve the presumption of innocence (Article 6 para 2).

5. *Privacy*: Automatic anonymisation

While using large amounts of data, at the same time, predictive models can based on databases from online sources that sufficiently anonymize their users, or the data can be pseudonymized-before they are used-and thus can still be used to identify patterns and predict future terrorist behaviour while maintaining privacy protections.[406]

6. *Accuracy*: Higher justification for an interference

Several features of AI systems can be used to sharpen the accuracy of decisions. The '*Recall*' function describes the percentage of times a model correctly identifies an event or person, and the '*Precision*' function describes the number of false alarms.[407] Such functions can improve the preservation of the human rights of affected individuals. They can be used to achieve more accurate results than human investigators. The better the predictive accuracy, the more effective counterterrorism becomes, as does privacy protection.[408] Similarly, they can assist in assessing

---

[402] Jigsaw (2016). 'The Redirect Method', www.redirectmethod.org (accessed 26.7.2022).
[403] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 10.
[404] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 26.
[405] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 27.
[406] United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021) 24.
[407] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 26.
[408] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 6, 18 f.

the proportionality of an action,[409] such as when the action under observation correlates with an appropriate action when compared to the threat-informed other data stored by the system. Other measures can modify models so that potential discrimination is actually mitigated.[410]

7. *Transparency*: Revealing and explaining the justification for a decision

Decisions made by humans may often not be understood. They, too, can be subject to prejudices or have a poor quality and simply give insufficient reasons. Of course, it becomes all the more tricky when algorithms make the decisions. For these to be tolerated, so that someone understands, for example, why they are not allowed to board a plane because an algorithm has put them on a no-fly list for terror suspects, the decision must be understandable.[411] This can be achieved by explaining the algorithm behind the decision in a simple way along with the decision, without revealing its internal process in detail (which is important for the secrecy of the investigative work). Another option is to supplement the decision with human supervision that provides and is accountable for a comprehensible decision rationale.[412] Qualitative and quantitative technical standards can measure the system's transparency.[413] Thus, in particular *predictability and explainability* are relevant features. While predictability measures the difficulty of predicting outcomes of the decision making progress, explainability measures the ability to explain the progress.[414] Both can be improved with each decision of the system.

In my opinion, a high-quality AI system can improve the transparency of decisions in the future. The data used for decision-making can be disclosed in detail, as can the parameters that led to the classification as a "danger" by simultaneously balancing the need for secrecy. In this context, an important advantage of AI techniques would be its potential to actually „*mitigate human bias in decision making*"[415] and thus to reveal existing discriminatory structures and

---

[409] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 26.
[410] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 16; also Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 26.
[411] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 84; Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 10
[412] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 84.
[413] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 28.
[414] Andrew Tutt, 'An FDA for Algorithms', 69 Admin. L. Rev. (2017) 102.
[415] Report by the Islamic Military Counter Terrorism, AI and Counterterrorism (2020) 9.

minimize them,[416] if data is selected not „*arbitrarily*“,[417] but *carefully*[418]. This level of accuracy requires resources not available in human work, while a system can be trained to automatically produce not only the decision, but also its comprehensible rationale. Even errors of the system can become transparent – more transparent than in human decisions – because the system can be trained to – unemotionally and without fear of the consequences – evaluate itself.

IX. Conclusions

The following summary refers to the research questions under II.6.

AI systems are suitable for the use in counterterrorism and can equally meet human rights standards. However, certain criteria have to be met. Any legal framework on the basis of which surveillance measures are implemented that are capable of interfering with the right to private life has to be clear and accessible and must pursue a legitimate aim in terms of Article 8 (2) ECHR (of particular importance: *national security, public safety and the prevention of crime*). Any measure based on that national law must be necessary in a democratic society in order to achieve those aims. In order to measure the necessity and the effectiveness of surveillance systems there should be regularly assessments carried out by a national independent supervisory body. To examine whether a measure is proportionate, according to the ECtHR case law a number of factors are relevant: such as the duration of the retention, the seriousness of the offence, the type of the data (the more intimate and intrusive, the higher the scrutiny), the age of the suspect and the existence of adequate safeguards.

Regarding gaps in the legal protection, in the majority of the analysed the ECtHR case law a violation of Article 8 ECHR was decided due to *insufficient safeguards*. The national legislator must take this into account: Adequate safeguards and guarantees against abuse are realized through determined legal criteria for measures, a limited use for the legitimate purposes of the retention, access only for specific authorities, and a (judicial) pre-authorization. Further, affected persons must be able to challenge the surveillance measure or its inclusion in a

[416] FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 103.
[417] United Nations General Assembly (2014), ‘Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age’.
[418] Janneke Gerards, Raphaële Xenidis, ‘Algorithmic discrimination in Europe’ (2020) 122.

database. The right to an effective remedy under Article 13 ECHR is fulfilled in particular by a review by an independent and impartial court. In this regard, the procedural guarantees of Article 6 ECHR must be assured. In doing so, the court must be competent to review the case in substance, including human rights violations. Further, the measures must not run the risk of *discriminating* against certain population groups. This goes both ways: The law must make justifiable distinctions; the data of convicted persons may be kept longer than the data of innocent persons. Further, the prohibition of discrimination must be taken into account in the collection of data for AI systems and in their processing and finally, the systems must be constantly checked for biases. Eventually, the lack of *transparency* is a problem that becomes particularly relevant in the case of an appeal against the decision, because the person concerned does not know on what basis his or her name was included in the database. This could be counteracted by easing the burden of proof (see Proposals, X.6.). Particularly relevant is therefore the *judicial review* of surveillance measures and the establishment of an independent *ombudsman*.

At the same time, AI systems can bring *benefits* with regard to the human rights protection of suspects. As has been argued, AI systems can improve the human rights situation if they are technically enabled to evaluate their own biases which can even reduce discriminatory decisions (Article 14 in conjunction with Article 8 ECHR). Moreover, the higher the technical standards and the quality of the databases, the sharper the pre-selection. Thus, AI systems can even make more accurate decisions than humans, resulting in a lower error rate and thus higher protection against unjustified actions. Therefore an interreference into the right to private life (Article 8 ECHR) could have a higher level of justification compared to a human decision. With appropriate features to explain the algorithms and decisions based on them, these systems can even provide more transparent outcomes than human decisions and therefore serve for a better ground to challenge the decision before the courts, which serves Article 6 and 13 ECHR.

In particular it has been shown that AI systems contribute to the the purpose of deradicalization: they are capable of filtering out people who are easily seduced into radicalization from social media and bringing them back to ‘the right path’. This could be an incredibly rewarding field of application for AI systems. Highlighted as an example is the *Redirect Method* which *redirects* users to ‘positive’ videos and messages which can provide for a credible counter-narrative to radical narratives. Automatic filtering of 'keywords' on social media linked to

extremist ideologies can also serve to identify the corresponding users in advance and direct them to 'positive' websites through algorithms or invite them into a deradicalization program.

X. Proposals

On the basis of the criteria according to the ECtHR case law (point VII), on the one hand, and the identified opportunities offered by AI systems on the other hand (VIII), as well as the conclusions drawn from them (point IX), an attempt is finally made to elaborate proposals.

1. Specialized investigation

As noted, there is often a lack of expertise in dealing with secrecy and technical issues.[419] This is particularly relevant with regard to the protection of privacy and the prevention of discrimination. Therefore a special authority may be established on the national level. It should be competent to authorize surveillance operations by the intelligence and the executive, in cases of imminent danger also ex post. Thus, it would be purposeful that it consists of experts in surveillance matters and human rights, in particular data protection law in the field of severe criminal offences and counter-terrorism. The FRA study justifies this primarily in order to avoid overlaps with traditional police activities.[420] However, an authorizing body and the operating police may be contemplating each other. In my view, the main reason for the establishment of such an authority is the need for special expertise both in the field of AI and terrorism and in the protection of human rights as well as a concentration of resources. A difference also lies in the orientation of the work. While police investigate suspicions of a crime that has already been committed, intelligence uses AI to try to detect and prevent future acts of terrorism.[421]

2. Specialized monitoring authorities

Both domestically and internationally, authorities must be able to review monitoring activities as quickly as possible and determine whether human rights standards have been met. For this reason a separate authority consisting of independent experts in the fields of severe crime and counter-terrorism as well as AI and data protection may be established.

---

[419] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 10, 12, 56.
[420] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 28 with reference to PACE (1999), p.2.
[421] In this respect also FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 28 with reference to Council of Europe (2016), 64

On the national level, any court could establish a *separate chamber* with independent and impartial judges on this topic, capable of reviewing a case in substance. This would also take into account the criteria of the ECtHR, which requires a judicial review. It would monitor AI-based decision-making processes in the public sector and could also serve as a complaints authority[422] and be competent to give expert opinions about AI systems and their algorithms accessible for any person or institution concerned. Further, the authority would be advisable to publish categories of potential danger (such as bias) and to classify the algorithms into these categories according to their conception and complexity. Most importantly, this chamber may be the first decision-making authority for complaints from individuals whose data is included in an algorithm-based system for predictive identification of terrorists or terrorist attacks.

In addition, it would be advisable to establish an *independent ombudsperson* responsible for complaints against surveillance measures. Its control would go beyond the individual case; the ombudsperson is to observe what need for improvement exists in the overall system. This ombudsperson can also conduct regular ad hoc reviews and additionally check both the laws and the measures for their compatibility with human rights standards. For the regular review, an additional independent *scientific expert council* can be established.

At the international level, it is worth considering setting up a *separate chamber directly at the ECtHR with experts* for this purpose, where such cases would be concentrated. It would be an advantage that the ECtHR already is competent to decide on complaints from individuals.

3. Special knowledge in AI and Human Rights

Combating new forms of terrorism cannot be done by criminologists alone; researchers from diverse disciplines such as psychology, security, communications, and computer science, must work together to develop appropriate systems to respond to terrorists' online activities ('*cognitive security*').[423] This comprehensive know how must be present at every level, in the production of AI systems used for counterterrorism, in the authorization of surveillance measures and in the review of measures. Who applies AI technologies needs to know how they function in order to evaluate the pre-decision, be aware of flaws as to issues like biases and take responsibility for the final decision. This applies to investigators; but even more to judges in order to be

[422] See for instance the proposal of Andrew Tutt, 'An FDA for Algorithms', 69 Admin. L. Rev. (2017) 118; supporting this idea Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung', JRP 26/2018, 12.
[423] Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014) 14 f.

able to justify the final decision on their own responsibility as well. [424] Therefore, there should be trainings in the field of the use of AI and human rights related issues.

4. International AI standards and clear legal framework in surveillance

On an international level, a repeated criticism is the absence of a comprehensive human rights guidance for the use of sensitive data in the context of counter-terrorism.[425] In particular, as the technical issues are highly complex and the surveillance legislation is considered complex,[426] an effective work in counterterrorism needs a clear and transparent legal framework and definitions. In the same way, the competences of the intelligence services must be clearly determined by law, flanked by safeguards against arbitrary action. Protection against abuse becomes all the more relevant the more secret the measures are. Therefore internationally acknowledged standards for the use of AI may contribute also to a harmonized protection of human rights standards as well as to international counterterrorism approaches.

5. International Ethical standards

For the same reasons (as mentioned in point 5) common ethical standards would improve the human rights situation in the field of counter-terrorism. As a model can serve the Ethical Guidelines of the AI Expert Group of the European Commission.[427] They emphasize the importance of building AI systems that are worthy of trust, '*since human beings will only be able to confidently and fully reap its benefits when the technology, including the processes and people behind the technology, are trustworthy*.' Thus, the expert group identified three elements of Trustworthy AI, whereby each of them is necessary but for itself not sufficient:[428]

1) it should be lawful, ensuring compliance with all applicable laws and regulations,
2) it should be ethical, ensuring adherence to ethical principles and values and
3) it should be robust, both from a technical and social perspective since to ensure that, even with good intentions, AI systems do not cause any unintentional harm.

---

[424] David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021) 16.
[425] Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 14.
[426] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 11.
[427] AI HLEG, ‚Ethics Guidelines' (2019) 35.
[428] AI HLEG, ‚Ethics Guidelines' (2019) 35.

Thereby it has been also criticized that the system itself does not produce *direct causalities*, but the connections are ultimately conclusions of correlations.[429] There is a connection between the lack of transparency, the causalities of a decision and biases. For example, if a system makes the decision to identify subject X as a terrorist, the subject can only prove bias on the part of the system if he knows how the algorithm works.[430] Also only in this case can he prove causality between the bias of the system and the decision to choose him. In the case of non-transparent systems, on the other hand, X cannot prove any gaps in the system, nor can he show whether a different set of data or a different algorithm would have produced a different result.

6. Transparency and procedural facilitations

The (lack of) transparency is an issue on every level - the AI system itself, the explainability of the algorithm, the choice of data collected, stored and used for the system, the decision-making process and the supervisory control. However, at the same time, a crucial question is the maintenance of the necessary secrecy. Technical tools can be improved in a way to balance the need for keeping the necessary secrecy and at the same time providing for easily accessible explanations of decisions. As mentioned, both *predictability and explainability* are relevant features of AI systems.[431] Therefore, AI tools could become less complex[432] or could provide for simplified and disclosed explanations[433] without jeopardizing the investigation. Also, a team consisting of multiple disciplines (law enforcement, psychology, medicine, IT) should be mandated to human rights[434] and ethical[435] trainings[436] to sharpen the tools to be more accurate while at the same time they consider the protection of the fundamental rights involved. The European Parliament also recommends a '*black box*' that records data about each transaction performed by the machine, including the steps and logic that led to its decisions.[437] That could be used later on to analyse flaws, reveal the decision-making process and evaluate it.

---

[429] Reinhard Klaushofer, ‚Die menschenrechtliche Dimension Künstlicher Intelligenz', ZÖR 74 (2019) 409.
[430] Andrés Páez, 'Negligent Algorithmic Discrimination', in Law and Contemporary Problems Vol. 84:19 (2021), 27.
[431] Andrew Tutt, 'An FDA for Algorithms', 69 Admin. L. Rev. (2017) 102.
[432] Human Rights Council, UNHCR Report (A/HRC/48/31) para 20, 56; FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 13.
[433] FRA, Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights, 2020), 13.
[434] See also CERD General Recommendation No. 36, 24.11.2020 (CERD/C/G/C/36), para 43 - preventing discrimination.
[435] Ethics guidelines for trustworthy AI (EU High-Level Expert Group on AI, 2019), 3.
[436] *McCann and Others v UK* App no. 18984/91 (ECtHR [GC 27.9.1995).
[437] Report of the European Parliament with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))P8_TA (2017) 0051 para 12.

Transparency, however, does not have to be necessarily related to technical transparency. An alternative way to establish trust of the society is to provide for a transparent and predictable legal framework on which predictive analysis is based on. Furthermore, clear responsibilities of oversight bodies would achieve a more coherent understanding about the measures.[438] On domestic level there should be authorities responsible for standard-settings for AI systems with regards to both features (predictability and explainability) and as well for complaints against decisions. The same seems to be necessary on an international level as there is no centralized authority[439] at the moment which would set minimum-standards for AI Systems.

A possibility to deal with this difficulty would be to implement or, when already existing, for courts to apply a rule that shifts the *burden of proof* from the plaintiff to the defendant.[440] The justification therefore lies in the lack of transparency which makes it impossible for the plaintiff to show the required evidence to prove biases that result in a discrimination, whereas the defendant has the access to the algorithm and therefore is able to prove, that the dataset or the algorithm was not biased. If on the defendants side it is too hard to prove that it was not biased, at least they have to prove their efforts to implement a system that avoids biases.[441]

Another possibility is to allow a kind of *prima facie evidence*.[442] The issue here would be not a detailed evidence, but rather about probability and plausibility. Thereby it could be sufficient for the plaintiff to prove that another system with a certain comprehensible and non-biased data set of good quality would not have reached the same result as the system in question.

7. Interconnection between public and private sector

At the broader level, combating terrorism requires a holistic approach that combines prevention in advance and conflict resolution in the event of a crisis. It is therefore appropriate for states to cooperate actively through the UN or other appropriate institutions.[443] Thereby one has to focus not only on law enforcement, but on the cooperation between international organizations and states, while addressing violent extremism conducive to terrorism as well as protecting

---

[438] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 28.
[439] See also Andrew Tutt, 'An FDA for Algorithms', 69 Admin. L. Rev. (2017) 104.
[440] See also in this direction Andrés Páez, 'Negligent Algorithmic Discrimination', in Law and Contemporary Problems Vol. 84:19 (2021), 28.
[441] Similar Andrés Páez, ‚Negligent Algorithmic Discrimination', in Law and Contemporary Problems Vol. 84:19 (2021), 29.
[442] In Austrian case law: 'Anscheinsbeweis'.
[443] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 40.

human rights.[444] As the Secretary-General emphasised, a '*united international community best allows for the provision of support to affected countries and fostering institutional and social resilience to terrorism*'.[445] In my view, this is all the more true in view of the rapid technological advances that are overcoming state borders as well as static legal systems.

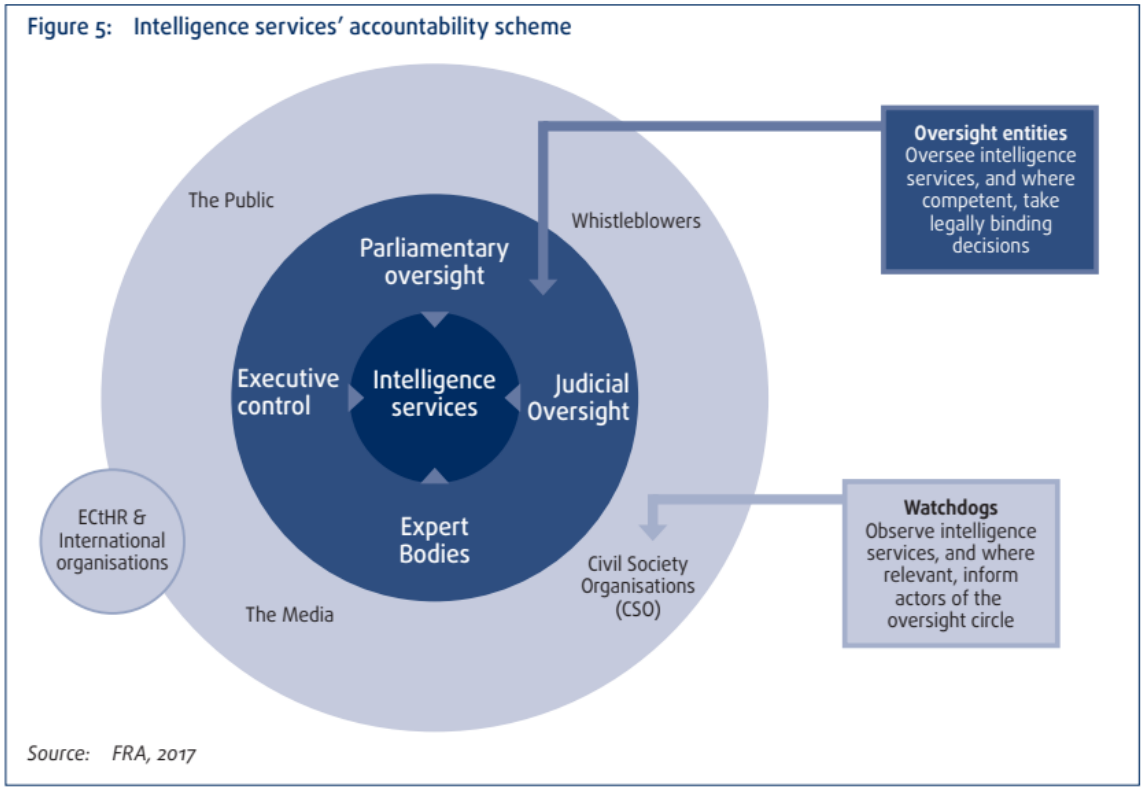
On the domestic level, an issue is the involvement of different sectors, public law enforcement and the private sector.[446] Following from the analysis, an interconnection between the sectors is necessary. The public sector alone cannot develop AI systems; it has to rely on corresponding companies with the technical expertise. In my opinion, the challenge, but also the innovation, would lie precisely in the networking of these sectors in the area of legal standards and expertise. Companies that focus on the development of AI for the criminal sector should also be familiar with human rights requirements and be obliged to adhere to them, while at the same time technical experts are also involved in the area of intelligence and law enforcement.

In this regard, the 73rd General Assembly in 2018[447] the Special Rapporteur on Human Rights underlines an inadequate engagement with relevant stakeholders before the adoption of the Resolution, in particular through independent experts and civil society with knowledge of human rights law and the lack of obligations to undertake a human rights impact assessment as well as monitoring mechanisms.[448] Accordingly, the effectiveness of accountability systems is enhanced by the involving a variety of stakeholders.[449] As key actors parliamentary bodies focus on the legality and functioning of the intelligence system,[450] while expert bodies[451] focus

---

[444] Ralph Janik, 'Terrorism' in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022) para 46.
[445] United Nations Secretary General, A/74/677 (2020) Activities of the United Nations, para 2.
[446] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 12 f.
[447] A/73/361.
[448] A/73/361 para 46 ff; also Krisztina Huszti-Orbán, Fionnuala Ní Aoláin, 'Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism' (2020) 11.
[449] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 135.
[450] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 76.
[451] Examples for them within the Member States are in Austria: Legal Protection Commissioner (Rechtsschutzbeauftragter), in Belgium: Standing Intelligence Agencies Review Committee (Vast Comité van Toezicht op de inlichtingen - en veiligheidsdiensten/Comité permanent de Contrôle des services de renseignement et de sécurité) Administrative Commission (Bestuurlijke Commissie/Commission Administrative), in Germany: G 10 Commission (G 10-Kommission) Independent Committee (Unabhängiges Gremium France - National Commission for Control of Intelligence Techniques (Commission nationale de contrôle des techniques de renseignement) Council of State special formation, in the Netherlands: The Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten), based on FRA 68. According to the FRA study expert bodies have the widest powers. In 22 Member States at least one non-judicial body has full access to

on specific operations and national human rights institutions, civil society organisations, ombuds institutions as well as media function as 'watchdogs'.[452] By launching lawsuits NGOs promote reforms and the development of case law and constantly act as watchdogs of the legislator.[453]



Source: European Union Agency for Fundamental Rights[454]

In addition to Figure 5, in my opinion, academia as well as private business are important key actors. The interconnectedness between all of these actors begins with the preparation of legislation, whereby key stakeholders should be involved in an open debate. According to the interviewed experts for the forementioned FRA study broader involvement of key actors and

the data collected, however, only in a few cases can decisions of non-judicial bodies be reviewed by a judge: see FRA 114.

[452] The FRA study also names whistleblowers (and describes them as Data protection authorities, which are treated as a type of expert body for purposes of this report): FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 65.

[453] See, for example, *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021); *Youth initiative for human rights v. Serbia* App No. 48135/06 (ECtHR 25 June 2013).

[454] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 114.

stakeholders in the development of intelligence legislation is needed.[455] Governments should collaborate with Human Rights Lawyers, AI (technical) experts and academics.

Recently, doubts arose about the fairness of commercially developed algorithms intended for police use or to serve as the basis for legal decisions.[456] From this it is clear that models developed by the private sector need to be assessed for their 'human rights compatibility', in particular their predictive accuracy, issues of proportionality and effectiveness need to be measured. Thus, the interlink should continue with the production of the models, regularly testing and evaluation obligations for developers as well as users of AI systems.

8. Responsibility of human decision-makers

Particularly in the context of counterterrorism, classification as a suspect can have serious consequences, ranging from a ban on boarding an airplane to possible restrictions on finding a job, and so on. Even with improved transparency, some opacity will remain simply because of the security risk and the concomitant need for secrecy. Some promotes the idea to delegate moral responsibility to the machines, making human control unnecessary.[457] However, it seems advisable to transfer the responsibility to a '*human controller*'. This person should make the final decision, not unlike other decisions made on the basis of documents and evidence. In this respect, the algorithm is not intended to replace humans as an independent decision-making authority, but to facilitate the decision as an automatic filter and additional evidence. An alternative way could be to establish always a '*human veto*'. So if a machine learning algorithm suspects someone is a terrorist, an investigator could overrule that decision.[458]

However, it should be taken into consideration that the AI system had at its disposal a myriad of data sets that were filtered by the algorithm and evaluated based on certain criteria. How can a human investigator rationally verify this? In my opinion, it is therefore primarily a matter of the explainability and comprehensibility of the decision-making process and the reasons for the decision that someone can recognize, understand and communicate to the outside world, in particular to the suspect concerned, and ultimately also have to take responsibility for.

---

[455] FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU' (2017) 11.
[456] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 21.
[457] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 43-46. He refers to research groups aiming to teach autonomous weapons systems ethics. There is, he follows, the hope that ethical machines will not violate democratic values such as necessity and proportionality and the prohibition of discrimination.
[458] Scott Alan Robbins, 'Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control' (2021) 44.

9. Higher standards for private business

Usually, the private sector has more possibilities, budget and discretion over how to build AI systems or even use the data of their customers.[459] As the GDPR notes, the '*exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased*.'[460] To some extent, law enforcement agencies are dependent on private companies for the budget and expertise to develop and advance AI systems. If companies are the bearers of the data, they can turn it into a 'commodity'[461] and sell the data collected, f.i. from the monitoring of telecommunications or social media, or even assessment results, to the public sector such as law enforcement, intelligence services. That has been reported to have happened with social media platforms as Twitter or Facebook.[462]

On the one hand, the value obtained by attracting companies is enormous and their work is extremely efficient. Thus, for instance, the mentioned project about the '*Redirect Method*' which aims to detect vulnerable persons before being seduced by extremist ideologies, is extremely valuable and has been created by the private company *Jigsaw* (see above VIII.4.). Also, as mentioned, the *INSIKT* which predictive analytics can provide insights into the network structure of terrorist groups and serve to reduce attacks (see above #) , is created by a start-up company. There are countless more examples of private business contributions in this field.

On the other hand, a challenge here is seen in a reduction of responsibility.[463] As private entities, companies are not directly subject to human rights obligations, neither internationally nor nationally (although the latter always depends on the respective concept of jurisdiction, but as a rule, companies are bound at best via a third-party effect of fundamental rights). A European digital rights initiative paper observes that the '*dangers of extra-judicial policing and punishment by private companies have not been assessed with regard to fundamental rights*.'[464]

---

[459] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 16.
[460] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Preamble para 5.
[461] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 17; see
[462] Matt Cagle, 'Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color', ACLU Northern California website, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target (accessed 19.7.2022).
[463] Kathleen McKendrick, 'Artificial Intelligence Prediction and Counterterrorism', The Royal Institute of International Affairs (2019) 17.
[464] See John McNamee, The Slide from 'Self-Regulation' to Corporate Censorship (01/2011) 3; available: https://www.edri.org/files/EDRI_selfreg_final_20110124.pdf (accessed 27.7.2022).

However, in my opinion, the advantages from the involvement of private companies are enormous: financial as well as human resources for the development of high-quality systems, among others also due to the competition on the market, usually better technical knowhow and deeper insights into the current - very rapid - developments in AI technology. Therefore, it is necessary to try to find a synthesis. There are currently no binding regulations for private companies to comply with human rights standards when developing AI systems.[465] As a first step, companies could be encouraged to comply with *soft laws*. Companies developing AI systems, especially if they are intended for use by public authorities (such as law enforcement and intelligence agencies), should at least consider soft law guidelines that provide a framework for companies to respect human rights. One model is the '*Civil Law Rules on Robotics*' by the EU Parliament.[466] This set of recommendations deals with the developments in the field of Artificial Intelligence and offers a Code of Conduct, including recommendations with regard to ethical aspects, principles of transparency and safety, controllability and accountability, as well as the reversibility of autonomous, algorithm-based decisions and actions.

Regarding facial recognition, in 2021 the Committee of Convention 108+ published Guidelines on Facial Recognition including e.g. a strict limitation by law of its use,[467] the necessity to establish supervisory authorities[468] and outline that developers should to ensure a high quality and accuracy of datasets through '*sufficiently testing their systems and identifying and eliminating disparities in accuracy, notably with regard to demographic variations in skin colour, age and gender, and thus avoid unintended discrimination*'.[469] Similarly the Guidelines of the European Protection Board emphasizes the importance of reliability and accuracy of the data.[470] That only proves that the private business as developers are a key actor with regard to the question of how to improve the situation on transparency, accuracy and non-discrimination.

---

[465] Separate from this is the scope of the GDPR, which also applies to companies too, but those that processes personal data as part of the activities of one of its branches established in the EU (GDPR Preamble para 17, Articles 1-3.) and does not - a step before - address the development of systems that are then used by public authorities.
[466] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25), Thursday 16 February 2017, published in the Official Journal of the European Union, 18.7.2018.
[467] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 6.
[468] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 8.
[469] Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021) 9.
[470] European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement - Version 1.0' (12 May 2022) 10 f.

At the same time, companies may create *diverse teams* for the development of AI models, in which *human rights experts are involved*, or by external experts offering specific *human rights training* in the companies. Of course, no company can be obliged to take such measures. However, government agencies could be required to purchase only those systems for monitoring that meet these requirements.

Finally, a simple but effective approach to solving this problem could be to *implement legislation that obliges public authorities to use systems that comply with human rights*. This would also indirectly bind companies automatically to higher human rights standards if they intend to sell their goods to state authorities as well.

XI. Bibliography

- **Literature**

1. Andrés Páez, ‚Negligent Algorithmic Discrimination‘, in Law and Contemporary Problems Vol. 84:19 (2021)

2. Andrew Tutt, ‘An FDA for Algorithms’, 69 Admin. L. Rev. (2017)

3. Azizan, Sofea Azrina, and Izatdin Abdul Aziz Aziz, Terrorism Detection Based on Sentiment Analysis Using Machine Learning’, Journal of Engineering and Applied Sciences 12 (2017/3)

4. Bart Elias, ‘Risk-Based Approaches to Airline Passenger Screening, Congressional Research Service Report’, (2014)

5. Ben Lutkevich, ‘natural language processing (NLP)’, SearchEnterpriseAI https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP (accessed 27.7.222)

6. Collin J. Bennett, 'The Council of Europe's Modernized Convention on Personal Data Protection. Why Canada Should Consider Accession', CIGI Papers No. 246 (November 2020)

7. Damien Van Puyvelde, Stephen Coulthart, M. Shahriar Hossain, 'Beyond the Buzzword: big data and national security decision-making' (2017)

8. Daniel L. Byman, Why lone wolves fail (published 16.6.2016), https://www.brookings.edu/blog/order-from-chaos/2016/06/16/why-lone-wolves-fail/

9. Dave Simonds, The Economist, 'People Can Now Be Identified at a Distance by Their Heartbeat', (published 23.1.2020) https://www.economist.com/science-and-technology/2020/01/23/people-can-now-be-identified-at-a-distance-by-their-heartbeat (accessed 30.3.2022)

10. David Leslie, Christopher Burr, Mhairi Aitken, Josh Cowls, Mike Katell, & Morgan Briggs, 'Artificial Intelligence, Human Rights, Democracy, and the Rule of Law' in Council of Europe's Ad Hoc Committee on Artificial Intelligence (ed.) (2021)

11. Eric Tlozek, Israel is using an algorithm to spot the next 'lone wolf terrorist', and soon other countries will too, abcnews (published 21.12.2018) https://www.abc.net.au/news/2018-12-22/israel-algorithm-to-predict-next-palestinian-lone-wolf-terrorist/10620900 (accessed 30.3.2022)

12. F. Johnson, M. Zheng, Y. Vorbyevaa, A. Gabriel, H.Qi, N. Velasquez, P. Manrique, D. Johnson, E. Restrepo, C. Song, S. Wuchty, 'New online ecology of adversarial aggregates: ISIS and beyond', Science 352(6292), (published 17.6.2016, http://science.sciencemag.org/content/352/6292/1459 (accessed 27.7.2022)

13. Gabriel Weimann, 'Virtual Packs of Lone Wolves', *Medium.com*, (published 25.2.2014) (https://medium.com/p/17b12f8c455a - accessed 9.7.2022)

14. Gabriel Weimann, 'New Terrorism and New Media', Wilson Center (2014)

15. Graham Greenleaf, 'RENEWING DATA PROTECTION CONVENTION 108: THE COE'S 'GDPR LITE' INITIATIVES', (2016) 142 Privacy Laws & Business International Report, 14-17 August (2017)

16. Janneke Gerards, Raphaële Xenidis, Algorithmic discrimination in Europe (2020)

17. John McNamee, The Slide from 'Self-Regulation' to Corporate Censorship (01/2011) 3; available: https://www.edri.org/files/EDRI_selfreg_final_20110124.pdf (accessed 27.7.2022)

18. Josh Horwitz, "Facebook Says It Can Stop the Sharing of Most Terror-Related Posts within an Hour of Creation." Quartz, 29.11.2017, https://qz.com/1140539/facebook-says-its-able-tostop-the-sharing-of-most-isis-terror-posts-withinan-hour-of-creation/ (accessed 21.7.2022)

19. Kaya Ismail, AI vs. Algorithms: What's the Difference?, CMS Wire (published 26.10.2018), https://www.cmswire.com/information-management/ai-vs-algorithms-whats-the-difference/ (accessed 23.7.2022).

20. Kathleen McKendrick, Artificial Intelligence Prediction and Counterterrorism, The Royal Institute of International Affairs (2019)

21. Maggie Gray, Amy Ertan, Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment (2021)

22. Mark D. Chang, 'Trolling new media: violent extremist groups recruiting through social media', Calhoun: The NPS Institutional Archive (2015)

23. Marwa Fatafta, Algorithms of Occupation: Use of Artificial Intelligence in Israel and Palestine in Jonathan Andrew, Frederic Bernard (Ed.) Human Rights Responsibilites in the Digital Age (2021)

24. Matt Cagle, ‘Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color’, ACLU Northern California website, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target (accessed 19.7.2022)

25. Michaela Wiegel, Eines der weitreichendsten Anti-Terror-Gesetze der EU https://www.faz.net/aktuell/politik/ausland/frankreich-setzt-im-anti-terror-kampf-auf-algorithmen-17464470.html

26. Molavi Ramak, ‚Künstliche Intelligenz – Entwicklung, Herausforderungen, Regulierung‘, JRP 26/2018, 7

27. Laurence H. Silberman, Charles S. Robb, ‘The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction’ (2005)

28. Nikolay Radulov, ‘Artificial Intelligence and Security. Security 4.0.’, International Scientific Journal “Security & Future” 2019, 4

29. Ralph Janik, ‘Terrorism‘ in Christina Binder, Manfred Nowak, Jane A. Hofbauer, Philipp Janig (Hrsg.), Human Rights (2022)

30. Reinhard Klaushofer, Die menschenrechtliche Dimension Künstlicher Intelligenz, ZÖR 74 (2019) 407

31. Scott Alan Robbins, ‘Machine Learning and Counter-Terrorism: Ethics, Efficacy, and Meaningful Human Control’ (2021)

32. Stefan Luber, Nico Litzel, ‘Was ist Deep Learning?’, Big Data Insider, (published 26.4.2017) (https://www.bigdata-insider.de/was-ist-deep-learning-a-603129/ - accessed 6.7.2022)

33. Susie Allegre. ‘Rethinking Freedom of Thought for the 21st century’, European Human Rights Law Review, 3 (2017)

34. Verónica Dahl in Emilia Gómez (ed.) 'Assessing the impact of machine intelligence on human behaviour: an interdisciplinary endeavour' (2018)

35. Walid Magdy, Kareem Darwish, and Ingmar Weber, '#FailedRevolutions: Using Twitter to Study the Antecedents of ISIS Support', Association for the Advancement of Artificial Intelligence (2015), https://arxiv.org/pdf/1503.02401.pdf (accessed 27.7.2022)

- **Reports and Studies**

36. AI HLEG, 'A Definition of AI: Main Capabilities and Disciplines' (2019)

37. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, 'Guidelines of Facial Recognition' (28 January 2021)

38. CTCD, 'Analytical Brief: Biometrics and Counter-Terrorism' (2021)

39. OSCE Consolidated Framework for the Fight against Terrorism, PC.DEC/1063, Decision No. 1063, 934th Plenary Meeting (7 December 2012) Annex; published: https://www.osce.org/files/f/documents/7/5/98008.pdf (accessed 6.8.2022)

40. Institute for Economics & Peace, Global Terrorism Index 2022, Measuring the Impact of Terrorism (2022) 14 – available: http://visionofhumanity.org/resources (accessed 7.8.2022).

41. European Data Protection Board, 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement - Version 1.0' (12 May 2022)

42. Ethics guidelines for trustworthy AI (EU High-Level Expert Group on AI, 2019)

43. Fundamental Rights Agency (FRA), ‘Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU’ (2017)

44. Fundamental Rights Agency (FRA), Artificial Intelligence and Fundamental Rights (EU Agency for Fundamental Rights (2020)

45. Ingeborg Zerbes et al, Untersuchungskommission zum Terroranschlag vom 02.11.2020, Geschäftszahl BMI: 2020-0.748.397 (10.2.2021) https://www.bmi.gv.at/downloads/Endbericht.pdf

46. International Institute for Counter-Terrorism, IDC Herzliya, „A New Study on Lone Wolf Terrorism in Israel“ (published 26.6.2018) https://www.ict.org.il/Article/2221/Lone_Wolf_Terrorism_Israel#gsc.tab=0

47. Krisztina Huszti-Orbán/Fionnuala Ní Aoláin, ‘Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?’ - Report - Special Rapporteur on human rights and fundamental freedoms while countering terrorism (2020)

48. LPD Wien, Aktueller Ermittlungsstand rund um den Terror-Anschlag am 2. November 2020 in Wien (published 13.11.2020), https://www.bmi.gv.at/news.aspx?id=2F4F4D5758556B416D79633D

49. Ministry of Public Security of Israel, „Study: Terrorists post info on social media before attacking“ (published 12.6.2018) https://www.gov.il/en/Departments/news/study_on_lone_wolf_terror_phenomena_120618

50. NATO Science and Technology Organization, ‘Science and Technology Trends 2020–2040

51. INTERPOL, ‘Preventing Terrorist Travel’, https://www.interpol.int/en/Crimes/Terrorism/Preventing-terrorist-travel (accessed 11.7.2022)

52. Office of Counter-Terrorism, Cybersecurity source: https://www.un.org/counterterrorism/cybersecurity (accessed 15th April 2022)

53. Österreichischer Rat für Robotik und Künstliche Intelligenz (2018)

54. Report by the Islamic Military Counter Terrorism, Artificial Intelligence and Counter-terrorism Limitations, Opportunities and Risks (2020)

55. Report of the European Parliament with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))P8_TA (2017) 0051

56. United Nations Office of Counter-Terrorism, Algorithms and Terrorism: The malicious use of Artificial Intelligence for terrorist purposes (2021)

57. United Nations Office of Counter-Terrorism, 'Countering Terrorism Online with Artificial Intelligence', (2021)

- **Newspapers and other Websites**

58. Amos Harel, Second Terror Attack in a Week Reflects Israeli Intel's Shortcomings (published 28.3.2022), https://www.haaretz.com/israel-news/.premium.HIGHLIGHT-after-terror-attack-israel-needs-to-figure-out-if-this-is-part-of-something-bigger-1.10702333 (accessed 30.3.2022)

59. Bernard Marr, How Robots, IoT And Artificial Intelligence Are Transforming The Police, *Forbes*, (published 19.9.2017) (https://www.forbes.com/sites/bernardmarr/2017/09/19/how-robots-iot-and-artificial-intelligence-are-transforming-the-police/?sh=50710b485d61 - accessed 8.7.2022)

60. Caitlin Dewey, Al-Qaeda's Inspire magazine celebrates Boston bombings, *The Washington Post* (published 31.5.2013) (https://www.washingtonpost.com/news/worldviews/wp/2013/05/31/al-qaedas-inspire-magazine-celebrates-boston-bombings/ - accessed 9.7.2022)

61. Chris Baraniuk, ‘Durham Police AI to help with custody decisions’, BBC, 10.5.2017 (https://www.bbc.com/news/technology-39857645 - accessed 8.7.2022)

62. Dan Williams, „Europe Looks Towards Israel for Anti-terror Technology“, Haaretz (published 19.7.2016) https://www.haaretz.com/israel-news/europe-looks-towards-israel-for-anti-terror-technology-1.5412900 (accessed 30.3.2022)

63. Hadas Gold, Five people shot dead near Tel Aviv, the third attack in Israel in a week, CNN (published 30.3.2022), https://edition.cnn.com/2022/03/29/middleeast/shooting-near-tel-aviv-intl/index.html

64. Michael Cooper, Michael S. Schmidt/Eric Schmitt, Boston Suspects Are Seen as Self-Taught and Fueled by Web (23.4.2013), https://www.nytimes.com/2013/04/24/us/boston-marathon-bombing-developments.html

65. Richard Valdmanis, Boston bomb suspect influenced by Al Qaeda: expert witness, *Reuters* (published 23.3.2015) (https://www.reuters.com/article/us-boston-bombings-trial-idUSKBN0MJ0Z620150323 - accessed 9.7.2022); generally about the magazine Inspire

66. Facebook Statistics and Trends, *Datareportal* (https://datareportal.com/essential-facebook-stats#:~:text=Facebook%20had%202.936%20billion%20monthly,'active'%20social%20media%20platforms – accessed 9.7.2022)

67. Jigsaw (2016). ‘The Redirect Method’, www.redirectmethod.org (accessed 19.7.2022)

68. RED-Alert Homepage: https://cordis.europa.eu/project/id/740688/de (accessed 26.7.2022)

- **Case Law**

1. *Akgün v. Turkey* App no 19699/18 (ECtHR 20 July 2021)
2. *Albert and Le Compte v Belgium* App nos 7299/75 and 7496/76 (ECtHR 10 February 1983)
3. *Amann v. Switzerland* App no. 27798/95 (ECHR [GC], 16 February 2000)
4. *Antović and Mirković v. Montenegro*, App no. 70838/13 (ECtHR 28 February 2018)
5. *Aycaguer v. France* App no o. 8806/12 (ECtHR 22 June 2017)
6. *Barberà, Messegué and Jabardo v. Spain* App no. 10590/83 (ECtHR 6 December 1988)
7. *BB v France* App no 5335/06 (ECtHR, 17 March 2010)
8. *Benedik v. Slovenia* App no. 62357/14 (ECtHR 24 July 2018)
9. *Biao v Denmark* App no 38590/10 (ECtHR [GC] 24 May 2016)
10. *Big Brother Watch and Others v The United Kingdom* App no 58170/13 (ECtHR [GC] 25 May 2021)
11. *Bochan v. Ukraine* (no. 2) App no 22251/08 (ECtHR [GC], 5 February 2015)
12. *Breyer v. Germany* App no. 50001/12 (ECtHR 30 January 2020)
13. *Bryan v The United Kingdom* App no 19178/91 (ECtHR 22 November 1995)
14. *Carson and others v The United Kingdom* App no 42184/05 (ECtHR [GC] 16 March 2010)
15. *Catt v. the United Kingdom* App no 43514/15 (ECtHR 24 January 2019)
16. *Centrum för Rättvisa v Sweden* App no 35252/08 (ECtHR [GC] 25 May 2021)
17. *Chahal v The United Kingdom* App no 22414/93 (ECtHR 15 November 1996)
18. *Choreftakis and Choreftaki v Greece* App no 46846/08 (ECtHR 17 January 2012)
19. *D.H. and Others v The Czech Republic* App no 57325/00 (ECtHR [GC] 13 November 2007)
20. *Denisov v Ukraine* App no 76639/11 (ECtHR [GC] 25 September 2018)
21. *Dolińska-Ficek and Ozimek v Po land* App nos 49868/19 and 57511/19 (ECtHR 8 November 2021)
22. *Dragan Petrović v. Serbia* App no no.75229/10 (ECtHR 14 April 2020)
23. *Driza v Albania* App no 33771/02 (ECtHR 13 November 2007)
24. *Edwards v The United Kingdom* App no 46477/99 (ECtHR 14 June 2002)
25. *Fabris v France* App no 16574/08 (ECtHR [GC] 7 February 2013)
26. *García Ruiz v Spain* App no 30544/96 (ECtHR 21 January 1999)
27. *Gardel v France* App no 16428/05 (ECtHR, 17 March 2010)

28. *Gaughran v. the United Kingdom* App no. 45245/15 (13 June 2020)
29. *Garnaga v. Ukraine* App no. 20390/07 (ECtHR 16 May 2013)
30. *Georgiadis v. Greece*, no. 21522/93 (29 May 1997)
31. *Guðmundur Andri Ástráðsson v Iceland* App no 26374/18 (ECtHR [GC] 1 December 2020)
32. *Hasan and Chaush v Bulgaria* App no 30985/96 (ECtHR [GC] 26 October 2000)
33. *Hirvisaari v Finland* App no 49684/99 (ECtHR 27 September 2001)
34. *Hoogendijk v the Netherlands* App no 58641/00 (ECtHR [dec] 06 January 2005)
35. *Huvig v France* App no 11105/84 (ECtHR 24 April 1990)
36. *Jėčius v Lithuania* App no 34578/97 (ECtHR 31 July 2000)
37. *Károly Nagy v Hungary* App no 56665/09 (ECtHR [GC] 14 September 2017)
38. *Kennedy v The United Kingdom* App no 26839/05 (ECtHR 18 May 2010)
39. *Klass and Others v Germany* App no 5029/71 (ECtHR 6 September 1978)
40. *Kudła v Poland* App no 30210/96 (ECtHR [GC] 26 October 2000)
41. *Le Compte Van Leuven and De Meyere v Belgium* App nos 6878/75 and 7238/75 (ECtHR 23 June 1981)
42. *Leander v Sweden* App no 9248/81 (ECtHR 26 March 1987)
43. *Lupeni Greek Catholic Parish and others v Romania* App no 76943/11 (ECtHR [GC] 29 November 2016)
44. *M.K v France* App no. 19522/09 (ECtHR 18 April 2013)
45. *M.S. v. Sweden* (Report of the Commission, 11 April 1996)
46. *Mastromatteo v Italy* App no 37703/97 (ECtHR [GC] 24 October 2002)
47. *MB v France* App no 22115/06 (ECtHR, 10 May 2010)
48. *McCann and others v The United Kingdom* App no 18984/91 (ECtHR [GC] 28 September 1995)
49. *Mehmet Hasan Altan v Turkey* App no 13237/17 (ECtHR 10 September 2018)
50. *Mockutė v. Lithuania* App no. 66490/09 (ECtHR 27 February 2018)
51. *Molla Sali v Greece* App no 20452/14 (ECtHR [GC] 19 December 2018)
52. *Nada v. Switzerland* App no 10593/08) (ECtHR [GC], 12 September 2012)
53. *Naït-Liman v Switzerland* App no 51357/07 (ECtHR [GC] 15 March 2018)
54. *Oleksandr Volkov v Ukraine* App no 21722/11 (ECtHR 9 January 2013)
55. *Öneryildiz v Turkey* App no 48939/99 (ECtHR 30 November 2004)
56. *Osman v The United Kingdom* App no 87/1997/871/1083 (ECtHR 28 October 1998)

57. *P.N. v. Germany*, 2020 (§§ 87-90).
58. *Peck v. the United Kingdom* App no. 44647/98 (ECtHR 28 January 2003)
59. *Peruzzo and Martens v. Germany* app no 7841/08 and 57900/12 (ECtHR-V 4 June 2013)
60. *Pocius v. Lithuania* App no 35601/04 (ECtHR 6 July 2010)
61. *PP.G. and J.H. v. the United Kingdom* App no 44787/98 (ECtHR-III 25. September 2001.
62. *Ramos Nunes de Carvalho e Sá v. Portugal* App nos. 55391/13, 57728/13 and 74041/13 ([GC], 6 November 2018)
63. *Reczkowicz v Poland* App no 43447/19 (ECtHR 22 July 2021)
64. *Regner v The Czech Republic* App no 35289/11 (ECtHR [GC] 19 September 2017)
65. *Rotaru v Romania* App no 28341/95 (ECtHR [GC] 4 May 2000)
66. *S and Marper v The United Kingdom* App nos 30562/04 and 30566/04 (ECtHR [GC] 4 December 2008)
67. *Şahin Alpay v Turkey* App no 16538/17 (ECtHR 20 June 2018)
68. *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* App no. 931/13 (ECtHR [GC] 27 June 2017)
69. *Schwabe and MG v Germany* App nos 8080/08 and 8577/08 (ECtHR 1 March 2012)
70. *Selahattin Demirtaş v Turkey (No 2)* App no 14305/17 (ECtHR [GC] 22 December 2020)
71. *Segerstedt-Wiberg and Others v. Sweden*, App no 62332/00 (ECtHR 6 June 2006)
72. *Stec and Others v The United Kingdom* App nos 65731/01 and 65900/01 (ECtHR [GC] 12 April 2006)
73. *Suominen v Finland* App no 37801/97 (ECtHR 1 July 2003)
74. *Suprunenko v Russia* App no 8630/11 (ECtHR 19 June 2018)
75. *Szabo and Vissy v. Hungary* App no 37138/14 (ECtHR 12 January 2016)
76. *Tagayeva and Others v Russia* App no 26562/07 and 6 others (ECtHR 18 September 2017)
77. *Trajkovski and Chipovski v. North Macedonia* App nos. 53205/13 and 63320/13 (ECtHR 13 June 2020)
78. *Tsfayo v The United Kingdom* App no 60860/00 (ECtHR 14 November 2006)
79. *Užukauskas v. Lithuania* App no 16965/04 (ECtHR 6 July 2010)
80. *Uzun v Germany* App no 35623/05 (ECtHR 2 December 2010)

81. *Vasilev v. Bulgaria* App no 7610/15 (ECtHR 16 November 2021)
82. *Vicent Del Capo v Spain* App no 5527/13 (ECtHR 6 November 2018)
83. *Weber and Saravia v Germany* App no. 54934/00 (ECtHR [GC] 29 June 2006)
84. *Włoch v Poland* App no 27785/95 (ECtHR 17 January 2011)
85. *Youth initiative for human rights v. Serbia* App No. 48135/06 (ECtHR 25 June 2013)
86. *Z v Finland* App no 22009/93 (ECtHR, 25 February 1997)
87. *Zakharov v Russia* App no 47143/06 (ECtHR [GC] 4 Dec 2015)

- **Legal Instruments**

1. Human Rights Committee, CCPR/C/GC/36, General comment No. 36 (2018)

2. Human Rights Council, UNHCR Report (A/HRC/48/31)

3. Human Rights Council, 44th session, A/HRC/44/38, Extrajudicial, summary or arbitrary executions Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions (29 June 2020)

4. OHCHR, Human Rights Council, 27th session, A/HRC/27/37, The right to privacy in the digital age (2014)

5. Human Rights Council, UNHCR Report (A/HRC/48/31)

6. Committee on the Elimination of Racial Discrimination General recommendation No. 36, CERD/C/GC/36, 'Preventing and Combating Racial Profiling by Law Enforcement Officials' (24 November 2020)

7. Human Rights Council A/HRC/49/45

8. Office of the United Nations High Commissioner for Human Rights, Human Rights, Terrorism and Counter-terrorism, Fact-Sheet Nr. 32 (2008)

9. Security Council, resolution S/RES/1566 (2004)

10. In the 73rd General Assembly, A/73/361 (Advancing human rights through the mainstreaming of human rights in counter-terrorism capacity-building and technical assistance at the national, regional and global levels)

11. Human Rights Council, 16th Session (22/12/2010) A/HRC/16/51, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin - Ten areas of best practices in countering terrorism (Dec 2010)

12. UN Security Council S/RES/1373 (2001)

13. UN, Human Rights Council A/HRC/14/46 (2010), Report of the Special Rapporteur Martin Scheinin.

14. UN Security Council S/RES/2178 (2014)

15. UN Security Council S/RES/2396 (2017)

16. UN General Assembly A/RES/75/291

17. UN General Assembly A/RES/60/288.

18. United Nations General Assembly (2014), 'Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age'

19. HRCttee, CCPR/C/GC/36 (2018) General comment No. 36

20. OSCE/ODIHR, 'Human Rights In Counter-Terrorism Investigation' (2013)

21. Human Rights Committee, CCPR/C/GC/35 (2014), General Comment Nr 35, para 2 (with regard to Article 9 of the ICCPR).

22. Human Rights Committee, CCPR/C/GC/35 (2014), General Comment Nr 35

23. Human Rights Council, UNHCR Report (A/HRC/48/31)

24. CERD General Recommendation No. 36, 24.11.2020 (CERD/C/G/C/36)

25. UN General Assembly A/73/361

26. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25), Thursday 16 February 2017, published in the Official Journal of the European Union, 18.7.2018