The use of biometric surveillance in counter-terrorism: to what extent are basic human rights protected?

by Antonella Benedetto

ITSS Verona Magazine, Vol. 1, n. 2

Fall/Winter 2022

The use of biometric surveillance in counter-terrorism: to what extent are basic human rights protected?

Antonella Benedetto

To cite this article: Antonella Benedetto, *The use of biometric surveillance in counter-terrorism: to what extent are basic human rights protected?*, ITSS Verona Magazine, Vol. 1, no. 2, Fall/Winter 2022.

Keywords: security, surveillance, biometrics, counter-terrorism, human rights.

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: December 30th, 2022

Abstract: This paper addresses the use of biometric surveillance as a crucial counter-terrorism technique. Biometric technology is increasingly used to address transnational challenges in border management, law enforcement, intelligence and terrorism information gathering, particularly in the wake of 9/11. The adoption of biometric technology, according to a former Central Intelligence Agency (CIA) operations officer, "could help make America a safer place"[1] by protecting US civilians from terrorist threats. However, their use may also result in violations of fundamental human rights both by democratic governments, such as the United States of America, and also repressive, authoritarian regimes. This paper gives an overview of biometric technologies' legitimate use, and also analyzes their possible interference with fundamental human rights, especially in relation to the "Global War on Terror." This essay looks at the international legal system's regulatory responses to possible violations of human rights through biometric technology, and stresses how legislative gaps remain both at domestic and international level.

[1] John D. Woodward, "Biometrics: Facing Up to Terrorism" (RAND Corporation, 2001), 7, https://www.rand.org/pubs/issue_papers/IP218.html.

Biometric technologies are now an essential characteristic of contemporary law enforcement. Defined by the *MIT Technology Review* as "one of the top ten emerging technologies that will change the world",[2] biometric technologies are often recommended for their efficacy and accuracy. However, they have also been the target of serious controversy.[3] The United Nations Security Council's (UNSC) regulatory initiatives, such as Resolution 2396, are indicative of this trend. However, human rights analyses and recommendations on the use of biometric technology are still scarce and inadequate, despite the technology's quick progress and broad application.

Biometric technologies have frequently caused significant human rights issues for four main reasons. First, they can substantially compromise the right to privacy. Human rights scholars question whether some of these technologies, most notably live facial recognition in public places, can exist without threatening individuals' right to privacy and other interconnected rights, like the freedom of peaceful assembly. Secondly, there is a rising danger in deviating from the original purposes of biometric technologies, widening their use, for example, to monitor Covid-19 pandemic cases and people's movements. Third, biometric technology can reinforce racial, ethnic, gender, social class, and other disparities, and increase exclusion. Fourth, many governments rely on the private sector to develop and implement technologies for state surveillance. However, not all states can regulate or conduct business surveillance to the same extent.[4]

Biometric technology: definition, evolution and use

Despite the absence of a shared definition of "biometrics," this essay relies on the International Organization for Standardization's (ISO) definition of the term as an "automated recognition of individuals based on their biological and behavioural characteristics."[5]

---

[2] See note 1.
[3] Fieke Jansen, Javier Sánchez-Monedero, and Lina Dencik, "Biometric Identity Systems in Law Enforcement and the Politics of (Voice) Recognition: The Case of Siip," *Big Data & Society* 8, no. 2 (2021): 1, https://doi.org/10.1177/20539517211063604.
[4] Tomaso Falchetta, "The Use of Biometric Technologies for Counter-Terrorism Purposes in a Human Rights Vacuum," Just Security, December 20, 2021, https://www.justsecurity.org/79592/the-use-of-biometric-technologies-for-counter-terrorism-purposes-in-a-human-rights-vacuum/.
[5] International Org. for Standardization/International Electrotechnical Commission, "ISO/IEC TR 24741:2018 Information Technology — Biometrics — Overview and Application" (International Org. for

In some jurisdictions, biometrics have been defined more specifically. At the European level, "biometric data" falls under the definition of "special category data" within Article 4(14) of the General Data Protection Regulation (GDPR):[6]

> 'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data.

The physical characteristics considered as potential biometric identifiers include finger lengths, wrist and hand veins, knuckle creases, fingertip structure, hand topography, ear and lip shape; also voice patterns, retina scans, iris, and signature recognition.[7]

Traditional biometric techniques such as "shadowing" fingerprinting or identification by photographs have been used since the 19th century in former colonies and in criminal justice systems. However, usage has also been connected with gross violation of human rights: a remarkable example is the tattooing practice and identification cards adopted by the Nazi Regime to identify people of Jewish origin. Citizens' obligation to bring identity cards containing information about their ethnicity also played into the genocide in Rwanda.[8]

In China, the number of biometric sensors, cameras and scanners has increased dramatically in recent years, with the goal of monitoring citizens' movements and behaviour. This is particularly severe in regions of China such as the Xinjiang Uyghur Autonomous Region, as residents have seen the criminalization of fundamental rights in line with China's Counter-Terrorism Law,[9] in place

---

Standardization/International Electrotechnical Commission , February 2018), https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en.

[6] European Commision, 2018 Reform of EU data protection rules, May 25, 2018, Article 4(14), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN.

[7] Clifton L. Smith and David J. Brooks, *Security Science: The Theory and Practice of Security* (Amsterdam: Butterworth-Heinemann, 2013), 153-175, 164.

[8] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" (Human Rights Centre - University of Minnesota, 2020), 1-45, 5,https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf.

[9] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" (Human Rights Centre - University of Minnesota, 2020), 1-45, 6. https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf.

since the Islamic State Group (ISIS) executed its first Chinese citizen in 2015.[10] Additionally, mainland China's social credit system is based on this biometric information control mechanism.[11]

Europe is not exempt from these practices, either. In 2014, the Speaker Identification Integrated Project (SiiP) was launched to create an international and interoperable biometrics database at Interpol: now, it is the third-largest globally. However, this system has seen significant controversy. For instance, research on facial recognition algorithms has shown that they tend to make mistakes and perform worse on some groups, in particular black women, gender minorities, children and seniors, individuals with disabilities, and manual labourers.[12]

To what extent is it legitimate to use biometric surveillance to enforce the law? Besides the soft-law "UN Code of Conduct for Law Enforcement Officials",[13] at the regional level, the "European Code of Police Ethics"[14] defines law enforcement as:

> Police forces or police services, or other publicly authorised and/or controlled bodies with the primary objectives of maintaining law and order in civil society and, who are empowered by states to use force and/or special powers for these purposes […] and protecting the fundamental rights of the individual [Recommendation Rec (2001)10].

So, law enforcement agencies (LEAs) must protect and respect the individual's fundamental rights and freedoms in fulfilling the duties imposed upon them by law. According to the "Siracusa Principles": "respect for human rights is part of public order."[15]

The US case study

The Counter-terrorism Committee Executive Directorate (CTED) noted, in its December 2021 analytical briefing, that "the use of biometrics for counter-terrorism purposes - notably in the

---

[10] Shannon Tiezzi, "ISIS: Chinese Hostage 'Executed,'" The Diplomat, November 19, 2015, https://thediplomat.com/2015/11/isis-chinese-hostage-executed/.
[11] Bazina Olga, "Human Rights and Biometric Data. Social Credit System," *Przegląd Europejski*, no. 4 (2020): 39–50, 39. https://doi.org/10.31338/1641-2478pe.4.20.3.
[12] Jansen, Sánchez-Monedero, and Dencik, "Biometric Identity Systems in Law Enforcement," 1.
[13] General Assembly resolution 34/169, "Code of Conduct for Law Enforcement Officials," OHCHR. Accessed November 5, 2022, https://www.ohchr.org/en/instruments-mechanisms/instruments/code-conduct-law-enforcement-officials.
[14] Committee of Ministers of the Council, "The European Code of Police Ethics," September 19, 2001, 7. https://polis.osce.org/european-code-police-ethics.
[15] American Association for the International Commission of Jurists (AAICJ), Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (New York, 1985), Section B, iii(2), 5. https://www.icj.org/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf.

context of border management and security - has become increasingly widespread."[16] The massive use of biometric surveillance in preventing counter-terrorism and violent extremism has been largely driven by the US response to 9/11 with the "Global War on Terror." In 2002, a US House of Representative affirmed that the hijackers' activities could have been previously identified if information technology had been adopted before the attack on the Twin Towers.

In the aftermath of 9/11, the RAND Corporation issued a paper that encouraged the use of biometric technologies to prevent terrorist attacks in the future, making the US a "safer place". In particular, checks would be concentrated on airport facilities, identity theft and fraud in travel documents, and suspected terrorists' identification throughout the "FactCheck" application.[17] In 2003, the US Department of Homeland Security (DHS) awarded Accenture to develop the "US-VISIT program" (United States Visitor and Immigrant Status Indicator Technology) within the framework of the "Smart Border Alliance". The program, worth $10 billion, aims to renovate all security systems of US air, land and sea ports of entry. The US-VISIT program, however, expands the use of integrated personal data in biometrics, a development that marks the beginning of a "new politics of surveillance", and biometrics' practically limitless use in terrorist detection and investigation.[18]

In 2003, US authorities and their allies started to collect biometric data on people in conflict zones, starting with Iraq. The success story convinced the US administration to also employ this strategy in Afghanistan. By the end of 2019, the US and American allies had gathered biometric data on almost 7.5 million individuals, focusing on males of fighting age between 15 and 64 years old. However, this practice is not exclusive to the US. A number of international humanitarian and development agencies also collect biometric data for various purposes. The United Nations High Commissioner for Refugees (UNHCR) gathers data from Somali refugees; the International Organization for Migration (IOM) installed a biometric scanner to collect fingerprints at Somalia's

---

[16] See note 4.
[17] Woodward, "Biometrics: Facing Up to Terrorism," 3-8.
[18] Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25, no. 3 (2006): 336–51, https://doi.org/10.1016/j.polgeo.2006.02.001.

border, while the African Union Mission to Somalia (AMISOM) trained the local police to use biometric registration.[19]

In the aftermath of 9/11, the UNSC adopted Resolution 1373, which calls for member states (MS), under Chapter VII of the UN Charter, to employ efficient border controls, controls over the issuing of identity papers and travel documents, and to stop the counterfeiting, forging, and fraudulent use of identity papers and travel documents, in order to prevent the movement of terrorists or terrorist groups.[20] The resolution also stresses the risk of human rights abuses in implementing counter-terrorism measures. However, it fails to make a recommendation on which measures the state should adopt.

Both governmental and intergovernmental agencies tend to focus on border surveillance: they do not just collect data but also create biometric traveller screening systems at the disposal of other states. Some examples are the "US Personal Identification Secure Comparison and Evaluation System" (PISCES), used in more than twenty-three countries. Also, the Migration Information and Data Analysis System (MIDAS), developed by IOM, is primarily used in Sub-Saharan Africa. Although they declare to promote the responsibility of use and respect for privacy, none of these organisations' literature stresses a human rights-based approach.[21]

What about human rights? Measures taken at different levels

Human rights and security are not mutually exclusive ideas or practices. Instead, they are essentially linked and intertwined concepts. Security without respect for human rights is a myth, "a colossus with clay feet."[22] The use of biometric surveillance has a substantial impact on fundamental human rights: the right to life, liberty, security, the right to be free from torture, cruel, inhuman or degrading treatment, a fair trial, privacy and family life, access to work and social

[19] Katja Lindskov Jacobsen, "Biometric Data Flows and Unintended Consequences of Counterterrorism," *International Review of the Red Cross* 103, no. 916-917 (2021): 619–52, https://doi.org/10.1017/s1816383121000928.
[20] United Nations Security Council (UNSC) Res 1373 (28 September 2001) UN Doc S/RES/1373, 1(g), 2. https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1373(2001)&Language=E&DeviceType=Desktop&LangRequested=False.
[21] Huszti-Orbán and Ní-Aoláin, "Use of Biometric Data," 8-9.
[22] Fionnuala Ní Aoláin, "How Can States Counter Terrorism While Protecting Human Rights?" *Ohio Northern University Law Review* 45 (2019): 389. https://doi.org/https://scholarship.law.umn.edu/faculty_articles/674.

security. UN institutions, such as the General Assembly (GA) and the Human Rights Council, have stressed how the right to privacy represents the foundations of a democratic society and all its attached rights, such as freedom of expression, movement, peaceful assembly, and association.[23] The UN Special Rapporteur mandate emphasized the phenomenon of "digital welfare dystopia": the risk of undermining the individual autonomy and choice of the most marginalized categories of people such as women, children, members of religious, ethnic, racial, sexual minorities or people particularly vulnerable such as poor, refugees, asylum-seekers or victims of armed conflict and violence.[24]

Another significant issue related to biometric surveillance is bias risks. Despite the fact that these technologies process information more rapidly, some studies have shown that most face recognition systems exhibit racial and gender bias, which results in less accurate identification of darker skinned people. In counter-terrorism, such as during screening at border checks or in the context of real-time monitoring, employing face recognition may result in false positives. Furthermore, even though these tools show insufficient sensitivity to culture and other differences in how people behave and react, they are increasingly used in law enforcement contexts to evaluate a person's facial expressions to determine the subject's emotional state, which is beyond the scope of counter-terrorism. Similar worries arise regarding accents which are not typical, usually belonging to racial or ethnic minorities.[25]

Numerous binding and non-binding instruments at the international level enshrine the right to privacy. According to Article 12 of the International Covenant on Civil and Political Rights (ICCPR) and article 12 of the International Declaration on Human Rights (UDHR):[26]

---

[23] Huszti-Orbán and Nì-Aoláin, "Use of Biometric Data," 18.
[24] Report of the United Nations High Commissioner for Human Rights, "The right to privacy in the digital age," (Geneva: Office United Nations General Assembly (A/HRC/48/31), 2021), 8. https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement.
[25] Huszti-Orbán and Nì-Aoláin, "Use of Biometric Data," 27.
[26] The United Nations, *Universal Declaration of Human Rights* (Paris: United Nations General Assembly, 1948), art.12, 4. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

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

At the regional level, the European Charter of Fundamental Rights (ECFR) complies with the UDHR definition, laying out the right to privacy and no interference within Article 52. Regardless, privacy is a "qualified" right. As a consequence, interference with privacy is lawful when it is rooted in law, necessary in a democratic society, and proportionate for the achievement of a legitimate aim--such as for a health crisis, terrorist attack, or crime prevention. In the October 2021 Human Rights Council Resolution, privacy is enshrined an "enabling" right, with the "Right to privacy in the digital age" document, "undermining the ability of people to [....] exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement."[27]

The right to privacy has been legally recognized a number of times, a good example being the "S and Marper v the United Kingdom" case adjudicated by the European Court of Human Rights (ECHR). According to the ECHR, it is a breach of the right to privacy to retain DNA samples of people who have been detained but later cleared or no longer face prosecution.[28]

With the emergence of "datafication",[29] protecting human rights in the context of preventing counter-terrorism remains a challenge for states and businesses. Indeed, lately, governmental authorities increasingly rely on private companies to collect biometric information. At the international level, the "UN Guiding Principles on Business and Human Rights" (UNGPs) promoted by the Human Rights Council assess reliable global standards for preventing and fighting possible human rights violations connected with business activity.[30] These encourage adopting

---

[27] United Nations High Commissioner for Human Rights, "The right to privacy in the digital age," 7.
[28] S. and Marper v. the United Kingdom, JUSTICE (European Court of Human Rights 2008), accessed October 20, 2022, 7, https://rm.coe.int/168067d216.
[29] Jens-Erik Mai, "Big Data Privacy: The Datafication of Personal Information," *The Information Society* 32, no. 3 (2016): 192–99, https://doi.org/10.1080/01972243.2016.1153010.
[30] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, "Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework" (Geneva: UN Human Rights Council, 2011), https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

public policies endorsing responsibility to promote and respect individuals' privacy. Although not binding, they represent an essential step in addressing the human rights impact on corporate responsibility.

According to the Global Terrorism Index, in 2017, 68% of global terrorism was concentrated in just five countries: Iraq, Afghanistan, Nigeria, Syria and Pakistan.[31] Between 2011 and 2017, around 35,000 foreign terrorist fighters (FTFs) travelled to Iraq and Syria to join the Islamic State in Iraq and the Levant (ISIL/Da'esh) and other extremist groups. By November 2017, nearly 7,000 returned to their home countries.[32] UNSC Resolution 2396 (2017) is just one of the many thematic counter-terrorism resolutions shaped by UNSC Resolutions 2170 (2014) and 2178 (2014), requiring states to prevent the recruitment, departure, entry and transit of FTFs; and adopt the necessary legislation to prosecute persons who travel for participating or receiving terrorist training.

The 2017 Resolution focuses in particular on three points: improving the security of borders and aviation; prosecuting, rehabilitating and reintegrating FTFs; and better coordinating with the UN in supporting MS "for the purpose of preventing, detecting and investigating terrorist offences and related travel."[33] Although the Resolution invokes the "full respect for human rights and fundamental freedoms" in fighting terrorism, it lacks a comprehensive human rights perspective, as stressed by the "Special Rapporteur on Counterterrorism and human rights" report to the "73rd session of the General Assembly" (GA). The mandate of the Special Rapporteur highlighted that the Resolution adopted inadequate arrangements with relevant stakeholders, such as the UN human rights mechanism, other relevant civil society experts, and specialists of international and humanitarian and refugee law. The Resolution furthermore does not mention tools or instruments to monitor the human rights assessment about their implementation.[34] Moreover, less than a month

---

[31] START, "Global Terrorism Index 2019," 2019, https://www.economicsandpeace.org/wp-content/uploads/2020/08/GTI-2019web.pdf.
[32] Ní Aoláin, "How Can States Counter Terrorism While Protecting Human Rights?" 8.
[33] United Nations Security Council, "Resolution 2396 (2017) Adopted by the Security Council at its 8148th meeting, on 21 December 2017," (Distr.: General 21 December 2017), 7, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/460/25/PDF/N1746025.pdf?OpenElement.
[34] United Nations General Assembly, "Promotion and protection of human rights and fundamental freedoms while countering terrorism," (Distr.: General 3 September 2018), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/274/67/PDF/N1827467.pdf?OpenElement.

later, the US called for the adoption of a new Resolution to address the threat of foreign terrorist fighters.

The 2015 Madrid Guiding Principles implemented measures to stop the flow of FTFs contained in the UNSC Resolution 2178 (2014). Later, in the Addendum to the 2015 Madrid Guiding Principles (2018),[35] MS implemented the skills and capacity requirements of the UNSC Resolution 2396 (2017). These included maintaining, using and developing the biometric and data-sharing protocols; comparing the biometrics of nationals against other international biometrics databases; preventing attempts to impersonate other people; and finally adopting a clear human rights approach, taking into consideration also the rights of minorities, particularly the rights of children.[36] However, as noted by some countries such as Egypt and Uruguay, the Resolution lacks necessary support in terms of funding, technical assistance, and capacity-building implementation for MS. As a result, the UN, together with the Biometrics Institute, responded by publishing a "Compendium of Recommended Practices for the responsible use and sharing of biometrics in Counter-Terrorism."[37]

The main goal of this document is to provide MS "who may have little or no experience with biometric applications and may also face technical assistance and capacity-building challenges when implementing this technology."

The Compendium also aims to comply with the UNSC Resolution 2322 (2016), which calls on MS to share information, including biometric and biographic data, regarding FTFs and terrorist organizations to promote international law enforcement and judicial cooperation.[38]

---

[35] United Nations Security Council Counter-terrorism Committee. "Madrid Guiding Principles", 2018 Addendum (S/2015/939 and S/2018/1177), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf.

[36] Huszti-Orbán and Nì-Aoláin, "Use of Biometric Data," 4.

[37] United Nations, Biometric Institute, "Un Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism, (Security Council - Counter-Terrorism Committee (CTC)), 2018),https://www.un.org/securitycouncil/ctc/content/un-compendium-recommended-practices-responsible-use-and-sharing-biometrics-counter-0.

[38] Carolyn Allen, "Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism", (Biometrics Institute, 2022), https://www.biometricsinstitute.org/compendium-for-biometrics-in-counter-terrorism/.

States are approaching issues surrounding facial recognition use in diverging ways. In the past two years, Brazil increased the use of facial recognition software.[39] India plans to create a national facial recognition system: the "Aadhaar" database, the biggest in the world. In contrast, due to accuracy concerns and the possible negative impacts that these kinds of technologies can have on society, some US federal governments have applied moratoria on their use. California and some US cities such as San Francisco and Somerville, Massachusetts have already applied temporary utilisation restrictions. Morocco has followed the same path, based on respect for the national human rights obligations, while the last European Commission White Paper on AI imposed a 5-years moratorium.[40]

Conclusions

A single high-tech solution to combat terrorism does not exist. Over time, biometric technologies are becoming more and more pervasive in all aspects of our society. However, human rights legislative gaps concerning the use of biometric technology raise serious concerns: the use of these technologies increasingly compromises, both in democratic and autocratic governments, the right to privacy, freedom of expression and assembly. Democracies' need to control terrorism is consistent with the expansion of human rights discourse as a pillar of their foreign policy agendas. However, several counter-terrorism measures, including torture and inhumane and degrading treatment at borders or detention facilities, raise serious questions about human rights respect.

Therefore, regulatory attempts by the UNSC 2396 (2017) Resolution to require state cooperation on this are not surprising. However, the Security Council Resolutions do not provide technical details on how these obligations may be implemented to protect human rights, nor do MS have, in equal measure, adequate privacy and data protection legislation– in fact they frequently fail to establish and put in place the essential institutions to ensure comprehensive corporate

[39] Alessandro Mascellino, "Public Face Biometrics Increase in Brazil, Scrutinized for Biases, Rights Impact: Biometric Update," Biometric Update, June 13, 2022, https://www.biometricupdate.com/202206/public-face-biometrics-increase-in-brazil-scrutinized-for-biases-rights-impact.

[40] Huszti-Orbán and Nì-Aoláin, "Use of Biometric Data," 26.

accountability. According to Ní Aoláin,[41] the first simple but radical step in combating terrorism is to put human beings' worth and dignity at the centre of all laws and policies. The second is to integrate human rights into security frameworks. It is past time to abandon the counterproductive "trade-off" concept, as it is irrelevant to the long-term management of security and violence.

[41] Ní Aoláin, “How Can States Counter Terrorism While Protecting Human Rights?” 20.

Bibliography

Allen, Carolyn. “Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism.” (Biometrics Institute, 2022). https://www.biometricsinstitute.org/compendium-for-biometrics-in-counter-terrorism/.

Amoore, Louise. “Biometric Borders: Governing Mobilities in the War on Terror.” *Political Geography* 25, no. 3 (2006): 336–351. https://doi.org/https://doi.org/10.1016/j.polgeo.2006.02.001.

Bazina, Olga O. “Human Rights and Biometric Data. Social Credit System.” Przegląd Europejski, no. 4-2020 (2020): 36–50. https://doi.org/10.31338/1641-2478pe.4.20.3.

Council of Europe: Committee of Ministers, “Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics.” Council of Europe Publishing, 19 September 2001. https://www.refworld.org/docid/43f5c7944.html.

European Parliament And Council Of The European Union, Directive 95/46/EC (24 October 1995), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

Falchetta, Tomaso. “The Use of Biometric Technologies for Counter-Terrorism Purposes in a Human Rights Vacuum.” Just Security, December 20, 2021. https://www.justsecurity.org/79592/the-use-of-biometric-technologies-for-counter-terrorism-purposes-in-a-human-rights-vacuum/.

Ní Aoláin, Fionnuala. “How Can States Counter Terrorism While Protecting Human Rights?” Ohio Northern University Law Review, 45 (2019). https://scholarship.law.umn.edu/faculty_articles/674.

Huszti-Orbán, Krisztina, and Fionnuala Ní Aoláin. Rep. *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?* Human Rights Centre - University of Minnesota, 2020. https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf.

International Org. for Standardization/International Electrotechnical Commission. Tech. *ISO/IEC TR 24741:2018 Information Technology — Biometrics — Overview and Application*. International Org. for Standardization/International Electrotechnical Commission, February 2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en.

Jacobsen, Katja Lindskov. “Biometric Data Flows and Unintended Consequences of Counterterrorism.” International Review of the Red Cross 103, no. 916-917 (2021): 619–52. https://doi.org/10.1017/s1816383121000928.

Jansen, Fieke, Javier Sánchez-Monedero, and Lina Dencik. “Biometric Identity Systems in Law Enforcement and the Politics of (Voice) Recognition: The Case of SiiP.” *Big Data & Society* 8, no. 2 (2021): 1-13. https://doi.org/10.1177/20539517211063604.

Mai, Jens-Erik. “Big Data Privacy: The Datafication of Personal Information.” *The Information Society* 32, no. 3 (2016): 192–99. https://doi.org/10.1080/01972243.2016.1153010.

Mascellino, Alessandro. “Public Face Biometrics Increase in Brazil, Scrutinised for Biases, Rights Impact: Biometric Update.” Biometric Update, June 13, 2022. https://www.biometricupdate.com/202206/public-face-biometrics-increase-in-brazil-scrutinized-for-biases-rights-impact.

NÍ Aoláin, Fionnuala. “Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family : report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Fionnuala Ní Aoláin.” Geneva: UN Human Rights Council, 2021. https://policehumanrightsresources.org/report-of-the-special-rapporteur-on-the-promotion-and-protection-of-human-rights-and-fundamental-freedoms-while-countering-terrorism-fionnuala-ni-aolain-human-rights-impact-of-counter-terrorism-and.

Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, “Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework”, (Geneva: UN Human Rights Council, 2011). https://www.ohchr.org/sites/default/files/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

S. and Marper v. the United Kingdom, JUSTICE (European Court of Human Rights 2008). https://rm.coe.int/168067d216.

Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights (New York, NY: American Association for the International Commission of Jurists, 1984).

Smith, Clifton L., and David J. Brooks. *Security Science: The Theory and Practice of Security.* Amsterdam: Butterworth-Heinemann, 2013.

Special Representative of the Secretary-General. “Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy Framework. Human Rights Council, 2001. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

START. Rep. *Global Terrorism Index 2019*, 2019. https://www.economicsandpeace.org/wp-content/uploads/2020/08/GTI-2019web.pdf.

Tiezzi, Shannon. “ISIS: Chinese Hostage ‘Executed.’” *The Diplomat*, November 19, 2015. https://thediplomat.com/2015/11/isis-chinese-hostage-executed/.

United Nations Security Council (UNSC) Res 1373 (28 September 2001) UN Doc S/RES/1373, https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1373(2001)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 2170 (15 August 2014), UN Doc S/RES/2170, https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2170(2014)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) Res 2396 (21 December 2017), UN Doc S/RES/2396(2017), https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F2396(2017)&Language=E&DeviceType=Desktop&LangRequested=False.

United Nations Security Council (UNSC) (23 December 2015)(UNSC) Res S/2015/939, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/madrid-guiding-principles_en.pdf.

United Nations Security Council (UNSC) Res S/2015/939 S/2018/1177, (28 December 2018), https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-on-foreign-terrorist-fighters.pdf.

United Nations, *Universal Declaration of Human Rights* (Paris: United Nations General Assembly, 1948), https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

Woodward, John D. "Biometrics: Facing Up to Terrorism." RAND Corporation, 2001. https://www.rand.org/pubs/issue_papers/IP218.html.