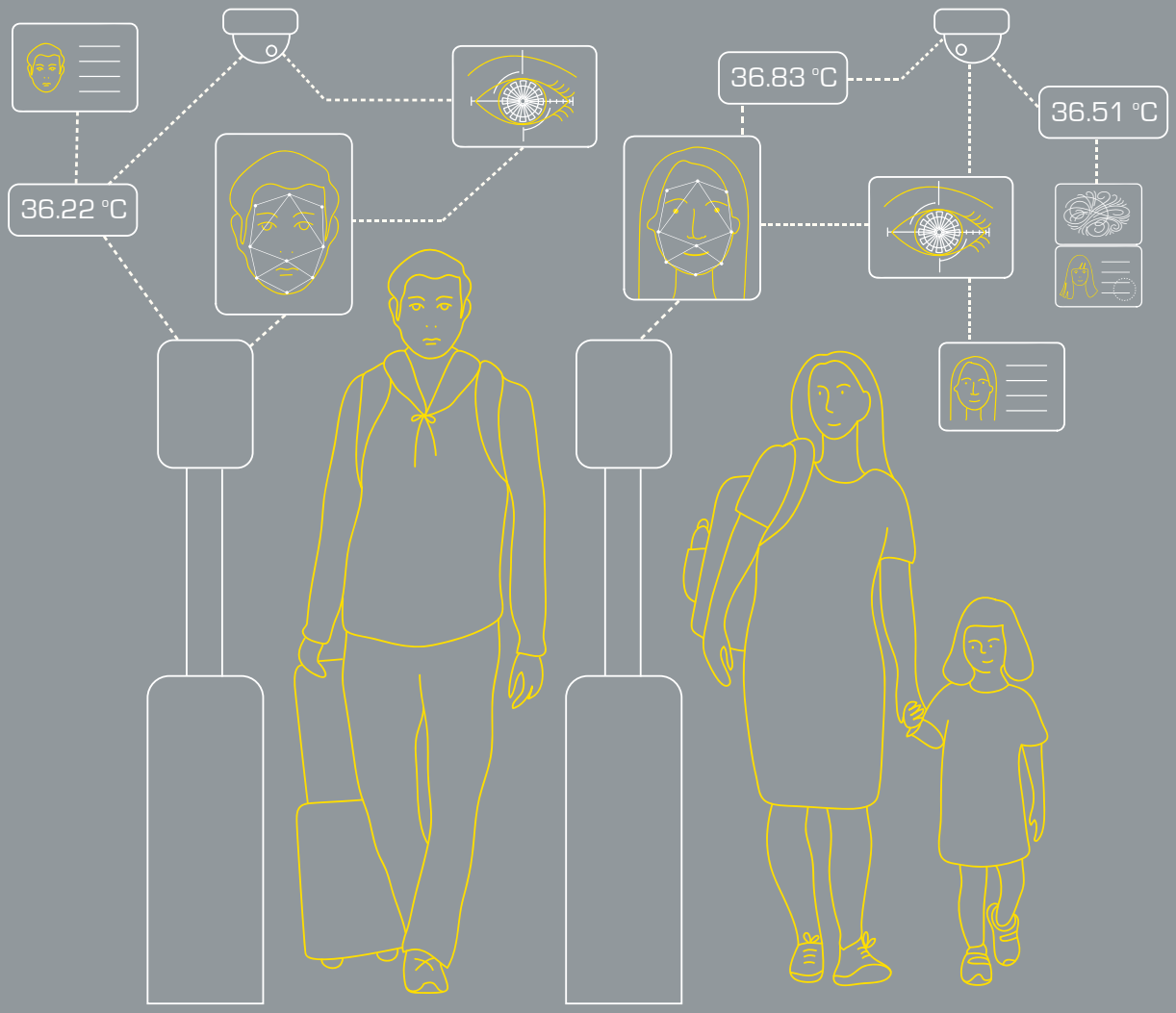
Border Management and Human Rights



Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context

OSCE ODIHR

Policy Brief: Border Management and Human Rights

Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context

30 YEARS OSCE ODIHR

Published by the OSCE Office for Democratic Institutions and Human Rights (ODIHR)

OSCE Office for Democratic Institutions and Human Rights (ODIHR)
Miodowa 10
00–251 Warsaw
Poland
Telephone: +48 22 520 06 00
Fax: +48 22 520 0605
Email: office@odihr.pl
osce.org/odihr

ISBN 978-83-66690-31-8

Design and illustration by V. Tzomaka.

Contents

Introduction

In a globalized world, more and more people cross international borders to develop and maintain personal contacts, pursue educational and professional opportunities, to migrate or to realize the right to seek asylum when fleeing from persecution.

At the same time, new technologies, which rely on the gathering, processing, and sharing of data, are increasingly used by states to manage migration flows and to address transnational security threats, including terrorism. These technologies heighten the risk of human rights breaches in an area that is already highly opaque and discretionary, with weak safeguards, accountability and oversight, and where the private sector plays a strong role in their development and use.

This policy brief, therefore, provides an overview of the implications of collecting and sharing information in the context of border management and how the introduction or continued use of new technologies in the border space may affect human rights. It also provides recommendations to OSCE participating States on how to respect and protect human rights when using new technologies to manage their borders. The policy brief has been prepared as part of the ongoing work of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) in the field of migration, freedom of movement, human rights and counter-terrorism.[1] More specifically, it is based on analysis from a series of online expert consultation meetings on new technologies in the context of border management and their impact on human rights, organized by ODIHR in June 2020, following a preliminary assessment that the increase in the use of new technologies for border management deserved attention, particularly considering potential human rights concerns.[2]

This policy brief references various digital technologies used in migration management and counter-terrorism, referring to passenger and biometric data collection, algorithmic decision-making, and artificial intelligence-based technologies as the innovations that are currently being developed and deployed for border and migration management, and to counter transnational organized crime and terrorism.

1 To learn more about ODIHR's work in these fields see, <https://www.osce.org/odihr/migration>; <https://www.osce.org/odihr/freedom-of-movement> and <https://www.osce.org/odihr/countering-terrorism>.

2 From 15 to 25 of June 2020, ODIHR organized a series of expert consultation meetings on "Border management and human rights: Collection and sharing of information and new technologies in the counter-terrorism and freedom of movement context" with over 80 participants in total. The series comprised four thematic session, which focussed on the human rights implications of: i) Advanced Passenger Information (API) and Passenger Name Record (PNR) systems, ii) the collection, storage and usage of biometric data in border management, iii) algorithmic profiling and decision-making in the border context; and iv) watchlists, databases and other information sharing for border security. Participants included the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (UN Special Rapporteur on counter-terrorism), the UN Special Rapporteur on the right to privacy, representatives from the Office of the High Commissioner for Human Rights (OHCHR), the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED), the OSCE, Council of Europe (CoE), EU Fundamental Rights Agency (FRA), Frontex, Interpol and other international institutions; participants from national border management agencies, as well as subject matter experts from civil society and academia. For more information on this event, see, <https://www.osce.org/odihr/453291>.

Border management, security and counter-terrorism

States have international obligations around border management in the context of countering terrorism. UN Security Council (UNSC) Resolution 2396 (2017) imposes legal obligations on states to establish systems for the collection, processing, and analysis of large amounts of personal data to detect terrorist travel and identify terrorists. Measures include systems for biometric data, Advance Passenger Information (API) and Passenger Name Records (PNR) as well as watchlists and databases of "known and suspected terrorists."[3] The resolution also encourages states to share this information with each other and with international organizations where appropriate.[4] OSCE Ministerial Council decisions call upon OSCE participating States to prevent the movement of terrorists, including so-called "foreign terrorist fighters,"[5] through effective border controls,[6] and to issue machine-readable travel documents that contain biometric data and take other measures to strengthen travel document security.[7] OSCE participating States have also committed specifically to establishing national API systems.[8]

States have a legitimate interest in controlling their borders and managing who enters their territory. But increased border security, including to counter terrorism, must not come at the expense of human rights and fundamental freedoms.[9] UN Security Council resolutions and OSCE commitments consistently reaffirm that all counter-terrorism actions must comply with international law, including international human rights and refugee law.[10]

At the 2005 Ministerial Council in Ljubljana, participating States reaffirmed their commitment to promote free movement of people across borders, while also pursuing the aim of reducing the threat of terrorism. They highlighted the need to treat individuals crossing borders with dignity in conformity with international and domestic law and human rights law. They also committed to increasing their efforts to ensure that national legislation, policies and practices provide to all persons equal and effective protection of the law and prohibit acts of intolerance and discrimination.[11] In line with these OSCE commitments, border management should not be linked to counter-terrorism measures based on assumptions about individuals or groups wishing to migrate.

---

3 UN Security Council (UNSC) Resolution 2396 (2017) paras 11-13 and 15. <http://undocs.org/S/RES/2396(2017)>.

4 *Ibid.*

5 The term "foreign terrorist fighters" has been subject to debate for its breadth and vagueness and the ensuing rights implications. For more information see ODIHR's, *Guidelines for Addressing the Threats and Challenges of 'Foreign Terrorist Fighters' within a Human Rights Framework*, 12 September 2018, <https://www.osce.org/odihr/393503>.

6 See, OSCE Ministerial Council (MC), Decision No. 5/14 "Declaration on the OSCE role in countering the phenomenon of foreign terrorist fighters in the context of the implementation of UN Security Council resolutions 2170 (2014) and 2178 (2014)", Basel, 5 December 2014, <https://www.osce.org/mc/130546>, OSCE MC Decision 1/01 "The Bucharest Plan of Action on Combatting terrorism", 4 December 2001, <https://www.osce.org/atu/42524>.

7 OSCE MC Decision No. 7/03 "Travel Document Security", Maastricht, 1-2 December 2003, <https://www.osce.org/mc/18445> and OSCE MC Decision No. 4/04 "Reporting List/Stolen Passports to Interpol's Automated Search Facility/Stolen Travel Document Database (ASF-STD)", Sofia, 7 December 2004, <https://www.osce.org/mc/16414>.

8 OSCE MC Decision No. 6/16 "Enhancing the Use of Advanced Passenger Information", Hamburg, 9 December 2016, <https://www.osce.org/cio/288256>.

9 See, OSCE MC Decision No. 2/05, "Border Security and Management Concept: Framework for Co-operation by the OSCE Participating States", Ljubljana, 6 December 2005, <https://www.osce.org/mc/17452>.

10 See, UNSC Resolution 2396 (2017); OSCE MC Decision No. 1/16 "Declaration on strengthening OSCE efforts to prevent and counter terrorism", Hamburg, 9 December 2016, <https://www.osce.org/cio/288176> and the 2012 OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063) <https://www.osce.org/pc/98008>.

11 OSCE MC Decision No. 2/05, Ljubljana, *op. cit.*, note 9.

Human rights most at stake

The OSCE comprehensive concept of security underlines the fact that effective counter-terrorism measures and human rights are not competing but mutually reinforcing objectives. Sustainable security requires the protection of human rights.[12] Ensuring security and protecting life is, in itself, a human rights commitment.

This policy brief will therefore highlight some of the human rights considerations that need to be borne in mind by states when using new technologies for border management and counter-terrorism.

General human rights principles: regulatory frameworks, effective remedies and oversight

International human rights standards allow restrictions of certain rights, such as the right to privacy and the right to freedom of movement, but only within strictly defined parameters. Any interference with those rights must be **prescribed by law, strictly necessary to achieve a legitimate aim, proportionate** towards the aim, and **not discriminatory**. States may not introduce restrictions that impair the essence of the right[13] in any circumstances. Similarly, there may never be any interference with **absolute rights and principles,** such as the **right to be treated with dignity and without discrimination** when crossing borders.[14]

International human rights law not only requires states to refrain from violating human rights but also **to protect individuals** from undue interference by others, including private persons and companies.[15] States must put in place **regulatory and institutional frameworks** to guarantee effective exercise of human rights in practice, including and especially in the border management and counter-terrorism contexts, given the unique and often highly discretionary decision-making context at and around the border. **Effective remedies and solid oversight and redress mechanisms**[16] are needed to ensure accountability and prevent violations of human

12 See, OSCE MC Decision No. 3/15 "Ministerial Declaration on Reinforcing OSCE Efforts to Counter Terrorism in the Wake of Recent Terrorist Attacks", Belgrade, 4 December 2015, <https://www.osce.org/cio/207261>. See also: OSCE MC Decision No. 3/07 "Ministerial Statement on Supporting the United Nations Global Counter-Terrorism Strategy", Madrid, 30 November 2007, <https://www.osce.org/mc/29544>. The 2012 OSCE Consolidated Framework for the Fight against Terrorism (PC.DEC/1063) identifies it as a strategic focus area to promote and protect human rights in the context of counter terrorism measures.

13 UN Human Rights Committee (CCPR), "General comment No. 31: The nature of the general legal obligation imposed on States Parties to the Covenant", 26 May 2004, CCPR/C/21/Rev.1/Add.13, para 6, <https://undocs.org/CCPR/C/21/Rev.1/Add.13>.

14 See OHCHR "Recommended Principles and Guidelines on Human Rights at International Borders", 2014, <www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_Guidelines.pdf>. OSCE participating States specifically committed to promote dignified treatment of individuals crossing borders, see OSCE MC Decision No. 2/05, Ljubljana, *op. cit.*, note 9.

15 With regards to private businesses, states should clearly set out the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations. In order to comply with corporate responsibilities to protect human rights, businesses should carry out human rights due diligence and impact assessments accordingly. See, UN Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", UN Doc. A/HRC/17/31, 23 March 2011, principles 2 and 17, <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>.

16 Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR) provides everyone whose rights or freedoms under the Covenant are violated the right to an effective remedy. For related OSCE commitments see also Concluding Document of Vienna – The Third Follow-up Meeting, 1989, para 13.9, <https://www.osce.org/files/f/documents/a/7/40881.pdf>; Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, 29 June 1990, para 5,5.10 and 5.11, <https://www.osce.org/files/f/documents/9/c/14304.pdf>; and Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE, 3 October 1991, para 18.2 and 18.4, <https://www.osce.org/odihr/elections/14310>.

rights. **Human rights education and training** of those involved in designing and implementing border control and counter-terrorism measures and making decisions in this space are an essential part of such a framework.[17]

The private sector plays an increasing role in the development and operation of border management systems powered by artificial intelligence and biometric technology, as key border management and security functions are being outsourced to private companies.[18] But effective state regulation and control in this field has not caught up with the pace of development. The regulatory and legal space around the use of new technology remains deficient, marked by discretionary decision-making, privatized development and uncertain legal ramifications.[19] **States are primarily responsible for ensuring respect for human rights and must put in place clear human rights based frameworks for the use of technology. The UN Guiding Principles on Business and Human Rights (the Ruggie Principles) also set out human rights responsibilities of businesses.** Businesses should exercise due diligence to avoid negative human rights impacts arising out of their activities.[20]

Border management and counter-terrorism technologies and systems can impact a wide range of human rights protected under international law. But some human rights are particularly relevant in this context:

Freedom of movement

Article 12 of the International Covenant on Civil and Political Rights (ICCPR) affords everyone the **right to leave any country, including his/her own, and the right to enter one's own country**.[21] Freedom of movement is an indispensable condition for the free development of a person.[22] While the entry of a non-national to the territory of a State may be subject to restrictions, any restrictions must be compliant with international human rights obligations. A **non-national may also enjoy the protection of the ICCPR in relation to entry or residence**, and any limitations on the right to freedom of movement must take account of other rights such as nondiscrimination, prohibition of cruel, inhuman or degrading treatment and respect for family life.[23]

---

17 In accordance with Article 2(1) ICCPR, states are required to adopt legislative, judicial, administrative, educational and other appropriate measures in order to fulfil their legal obligations under the ICCPR; see CCPR, General Comment No. 31, *op. cit.*, note 13, para 7. In addition, OSCE MC decisions refer to the provision of programmes that provide training on inter-alia non-discrimination and sharing of good practices in this area.

18 UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance (UN Special Rapporteur on racism), UN Doc. A/75/590, 10 November 2020, para 16, <https://undocs.org/en/A/75/590>, refers to the term "border industrial complex" which has been used to describe the growing privatization and securitization of border policing and migration management. See also UN Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (Working Group on the use of mercenaries), UN Doc. A/HRC/45/9, 9 July 2020, paras 75-77, <https://undocs.org/en/A/HRC/45/9>.

19 See Petra Molnar, "Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up", November 2020, EDRi and the Refugee Law Lab, <https://edri.org/wp-content/uploads/2020/11/Technological-Testing-Grounds.pdf>.

20 See UN "Guiding Principles on Business and Human Rights", *op. cit.*, note 15.

21 The right to leave any country may be subject to certain restrictions but only as far as the restrictions are provided by law, are necessary, proportionate and non-discriminatory. Regarding the right to return to one's own country, the CCPR also underlined that the meaning of "own country" is broader than the concept "country of nationality" and embraces also non-nationals with special ties to the country, such as long-term residents; see CCPR, General Comment No. 27: Article 12 (Freedom of Movement), UN Doc. CCPR/C/21/Rev.1/Add.9, 2 November 1999, <https://undocs.org/en/CCPR/C/21/Rev.1/Add.9>, para 20. Please also see the OSCE commitments on freedom of movement, Vienna 1989, *op. cit.*, note 16, para 20.

22 *Ibid.*, para 1.

23 CCPR, General Comment No. 15: The position of aliens under the Covenant, 11 April 1986, para 5. <https://www.refworld.org/pdfid/45139acfc.pdf>.

Right to seek asylum

The right to seek and enjoy asylum is enshrined in Article 14 of the Universal Declaration of Human Rights (UDHR) and further developed in the 1951 Refugee Convention and its Protocol.[24] The international protection framework of the Convention sets out the fundamental rights of refugees and related state obligations, including **the prohibition of forcible return** to a country where one's life or freedom would be threatened (**non-refoulement**).[25]

Equality and non-discrimination

Article 1 of the UDHR states that all human beings are born free and equal in dignity and rights. Article 2(1) of the ICCPR requires that states respect and ensure all rights recognized in the Covenant, "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status". Article 26 of the ICCPR guarantees equality before the law and equal protection by the law without discrimination.[26] States may not derogate from the principle of equality and non-discrimination even at times of public emergency.[27] **Discrimination is any distinction, exclusion, restriction or preference which is based on any ground such as those referred to above, and which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise of rights and freedoms by all persons.**[28] Border management may entail differences in treatment according to nationality, for example, but must not have a discriminatory effect. As will be discussed in further detail below, the use of new technologies to manage borders may indeed deepen racism, racial discrimination and xenophobia and lead to other forms of exclusion.[29] OSCE participating States have firmly rejected the identification of terrorism with any ethnicity, nationality, religion or belief and consistently reaffirmed the importance of equality and non-discrimination in countering terrorism.[30]

---

24 Convention relating to the Status of Refugees (hereafter Refugee Convention), 1951, <https://www.unhcr.org/3b66c2aa10>. Also see the OSCE commitments on asylum in the Istanbul Document, Charter for European Security, November 1999, para 22, <https://www.osce.org/files/f/documents/6/5/39569.pdf>.

25 1951 Refugee Convention, Article 33. The principle of *non-refoulement* is also enshrined in international human rights law, which prohibits the return of anyone to any country where he or she may be exposed to risks of torture or other serious human rights violations. The absolute prohibition of torture entails an absolute prohibition of *refoulement* to torture under all circumstances. For an overview see OHCHR "The Principle of *non-refoulement* under international human rights law", <https://www.ohchr.org/Documents/Issues/Migration/GlobalCompactMigration/ThePrincipleNon-RefoulementUnderInternationalHumanRightsLaw.pdf>.

26 In addition, the ICCPR specifically guarantees the equal rights of men and women (Article 3) and the rights of children to protection without discrimination on any ground (Article 24).

27 Including in relation to security threats or for the purposes of countering terrorism.

28 CCPR, General Comment No. 18: Non-discrimination, 10 November 1989, para 7, <https://www.refworld.org/docid/453883fa8.html>. For definitions of discrimination within the scope of the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), see article 1 of both Conventions.

29 UN Committee on the Elimination of Racial Discrimination (CERD), General recommendation No. 36: Preventing and Combating Racial Profiling by Law Enforcement Officials, CERD/C/GC/36, 24 November 2020, para 12, <https://undocs.org/CERD/C/GC/36>.

30 See e.g., OSCE Ministerial Council Decision, No. 1/01, Bucharest 2001, *op. cit.*, note 6; and the OSCE MC Decision 10/02, "OSCE Charter on Preventing and Combating Terrorism", Porto 2002, <https://www.osce.org/mc/42536>.

Right to privacy and data protection

The right to privacy is a **"gateway right"** – without privacy, the full enjoyment of a broad range of other rights is endangered. The right to privacy is guaranteed under Article 17 of the ICCPR. The **protection of personal data is an important element of the right to privacy** which is particularly relevant in the context of new technologies for border management and counter-terrorism.[31] **Key data protection principles** set out in international standards include that personal data undergoing automatic processing shall: (a) be obtained and processed fairly and lawfully; (b) be stored for specified and legitimate purposes, (c) be adequate, relevant and not excessive; (d) be accurate and, where necessary, kept up to date; and (e) be preserved for no longer than is required. **Sensitive data** (e.g., data revealing ethnic origin, political opinions, religious or other beliefs, health or sexual life, criminal conviction) requires a particularly high level of protection. Data security and protection against unauthorized access must be ensured; as well as the **right for the data subject to know that information is stored** on him or her, to have access to such data and to have it corrected, if necessary.[32] Participating States have committed to protect the right to private and family life, domicile, correspondence and electronic communications, as well as the prevention of arbitrary intrusion in the realm of the individual.[33]

Other rights

New technologies used at the border can also directly and indirectly affect a broad range of other rights; and it can directly and indirectly affect the rights of people in specific need of protection, such as refugees and asylum-seekers, children and victims of trafficking.[34] Depending on what decisions are taken and how they are taken in border management and security, the use of such technology can impact the **right to liberty, fair trial and due process standards**[35] such as the right to be heard; to a fair, impartial and independent decision-maker; to be provided with information and reasons for a decision and the right to appeal an unfavourable decision, among others. As will be discussed below, it can expose individuals to violations of the **absolute prohibition of torture and other cruel, inhuman or degrading treatment**[36] and lead to undue interferences with **freedom of religion or belief**.[37] But it can also indirectly affect a person's rights beyond the border context, for example through a chilling effect on the exercise of **freedom of expression, assembly and association**[38] and knock-on effects on many other rights.

---

31 See CCPR, General Comment No. 16: Article 17 (Right to privacy), 8 April 1988, para 10, <https://www.refworld.org/docid/453883f922.html>.

32 See Articles 5-8 of the Council of Europe "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (hereafter Convention 108), Strasbourg, 28 January 1981, Ref.: ETS No.108, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. In its interpretation of state obligations under Article 17 of the ICCPR, the UN Human Rights Committee recalled a number of corresponding data protection principles; see *Ibid.* CCPR, para 10. In the European Union, in addition to Article 8 of the EU Charter of Fundamental Rights, the more comprehensive set of principles contained in the EU General Data Protection Regulation (GDPR) also apply; see Regulation (EU) 2016/679, 27 April 2016, <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. The Convention 108 has been ratified by all of the 47 Council of Europe member states, i.e., the majority of OSCE participating States, and is also open for ratification by non-Council of Europe member states.

33 OSCE Moscow Document 1991, *op. cit.*, note 16, para 24 and Copenhagen 1990 for commitments related to access to information and protection of privacy, *op. cit.*, note 16, para 26.

34 As set out in the 1951 Refugee Convention; the Convention on the Rights of the Child (CRC); Article 8 of the ICCPR, which prohibits slavery and forced labour; and the Council of Europe Convention on Action against Trafficking in Human Beings, which seeks to protect victims of trafficking and safeguard their rights.

35 Articles 9 and 14 ICCPR as well as Article 2(3) providing, as noted before, for the right to an effective remedy against violations of one's rights to be determined by a competent judicial, administrative or legislative authority.

36 Article 7 ICCPR.

37 Article 18 ICCPR. The right to hold or adopt a religion or belief is absolute; only the right to manifest it can be subject to certain restrictions.

38 Articles 19, 21 and 22 ICCPR.

New technologies used for border management and impact on rights

Across the OSCE region, the implementation of new technologies and systems for collection and processing of personal data in border management and counter-terrorism is progressing to varying extents. This section provides a brief overview of the ways in which such systems and technologies can impact human rights.

Advance Passenger Information (API) and Passenger Name Records (PNR)

API is the biographic information stored on a travellers' passport.[39] It is collected by airlines at check-in and transmitted to border control and other relevant agencies of departure, transit and arrival countries, where such data-sharing across borders is permitted under applicable national law. Border agencies can use API data to complete automated searches, for example of INTERPOL databases. Usually, the data of all passengers on one flight is submitted to authorities at once in a single transmission. However, interactive Advanced Passenger Information (iAPI) forwards the passenger's information from the airline to the border agencies of departure and destination countries individually at the time of check-in. Border agencies may therefore respond in relation to individual passengers.[40]

PNR data is created during the purchase or booking of an airline ticket and can include passenger names, itinerary, ticketing information, meal and seat preference, general contact information and form of payment, as well as other information.[41] Unlike API, which is based on official travel documents, PNR data is entered manually by the traveller or the travel agent and therefore may not be accurate. It is stored by the airlines and shared with departure and arrival countries' border authorities before departure, unless there are any restrictions on sharing data due to national regulations or data protection standards.[42] States use PNR data to perform checks against other databases to identify "known or suspected" terrorists or criminals and to analyse the data for patterns that could reveal criminal behaviour. Border agencies can also respond to airlines regarding specific passengers before take-off.[43]

---

39 API data usually includes the surname/given names of the traveller, the nationality, date of birth, gender, official travel document number, issuing state or organisation, travel document type, expiration date.

40 For more details on format, technical standards and use of API, see, World Customs Organization (WCO), International Air Transport Association (IATA) and the International Civil Aviation Organization (ICAO), "Guidelines on Advance Passenger Information (API)", 2014, <https://www.icao.int/Security/FAL/SiteAssets/SitePages/API%20Guidelines%20and%20PNR%20Reporting%20Standards/API-Guidelines-Main-Text_2014.pdf>; and ICAO "ICAO TRIP Guide on Border Management Control", 2018, <https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf>. See also UN Security Council Counter-Terrorism Committee Executive Directorate (CTED) / UN Office of Counter-Terrorism (UNOCT) "United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism" (hereafter UN Compendium), 2018, <https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf>.

41 Whereas it is defined in national legislation and bilateral agreements what PNR data elements states require from carriers, the ICAO Guidelines on PNR Data contain a list of 19 categories of such data. See WCO/IATA/ICAO API Contact Committee "Air Transport & Travel Industry Principles, Functional and Business Requirements PNRGOV", 2013, p. 11, <https://www.icao.int/Security/FAL/Documents/2-PNRGOV-Principles_13-1version_FIRST.pdf>.

42 "UN Compendium", *op. cit.*, note 40, p. 59; C. Hanab, R. McGaurana and H. Nelen, "API and PNR data in use for border control authorities", Security Journal, Vol. 30, 2016, p. 1050.

43 WCO/IATA/ICAO API Contact Committee, *op. cit.*, note 41.

The collection and automated processing of API and PNR data by state authorities (through airlines) is a substantial interference with the right to privacy which, in order to be human rights compliant, must have a clear legal basis with appropriate safeguards; it must be necessary and proportionate to a legitimate aim; and must be non-discriminatory.

Data minimization, retention and protection of sensitive data

PNR data involves even more personal data being collected and processed than API; and it can be more intrusive and sensitive information, including private travel-related data, mobile phone, payment and credit card details. The collection and sharing of PNR affects the right to private life of anyone boarding an international flight.[44] Furthermore, sharing PNR data with government authorities for law enforcement purposes is quite different from the commercial purpose for which it was initially collected, therefore, raising questions around purpose limitation. Given the amount and type of data states require access to, and its effect on anyone travelling, concerns have been raised that PNR data collection and processing is untargeted, excessive and inconsistent with the principle that interferences must be minimized to the extent possible.[45]

PNR contains extensive information that could also reveal sensitive data for which the protection through appropriate legal safeguards has been recognized to be particularly important. This includes data revealing ethnic origin, political opinion, religion or belief, or information concerning health or sexual life, which might put people at risk of discrimination or other human rights abuses.[46] Even where PNR legislation provides that sensitive data may not be processed,[47] the risk remains that conclusions could be drawn, for example, from meal preferences regarding religious belief, or from travel history or co-travellers to someone's political opinions or sexual orientation.[48] Advance sharing of API or PNR data could lead to restrictions on freedom of movement for political dissidents, for example, or may prevent people from effectively seeking asylum.

---

44 The impact on people travelling across borders will be even more pervasive if API/PNR data is used also for other means of travel in the future, as it is being contemplated by the European Union. See e.g., Peter Teffer for EU Observer "EU may extend 'passenger name records' to rail and sea", Brussels, 6 August 2019, <https://euobserver.com/justice/145602>.

45 Critics have described it as "suspicionless mass surveillance" and challenged it before courts. See EDRI "ICAO mandates worldwide government surveillance of air travellers", 10 September 2020, <https://edri.org/our-work/icao-mandates-world-wide-government-surveillance-of-air-travelers/>. The PNR Directive was challenged before courts in Germany and Austria and is currently pending before the Court of Justice of the European Union (CJEU). See: EDRi "CJEU to decide on processing of passenger data under PNR Directive", 29 January 2020, <https://edri.org/our-work/cjeu-to-decide-on-processing-of-passenger-data-under-pnr-directive/>. For more information on the litigation see: <https://nopnr.eu/en/home/>.

46 Council of Europe "Convention 108", Article 6.

47 As prescribed, e.g., by the EU PNR Directive. See European Commission "Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", 4 May 2016, para 37 and Article 13, <http://data.europa.eu/eli/dir/2016/681/oj>.

48 Douwe Korff, "Passenger Name Records, data mining & data protection: the need for strong safeguards", Study prepared for the Council of Europe Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Consultative Committee of Convention 108), Strasbourg, 15 June 2015, p. 79 <https://rm.coe.int/16806a601b>. See also Evelien Brouwer "The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?", CEPS Working Document No. 320/ September 2009, p. 25, <http://aei.pitt.edu/11485/1/1903.pdf>.

There is no uniform approach to maximum storage time for API or PNR data in the OSCE region.[49] The Consultative Committee of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Consultative Committee of Convention 108) underlined that data retention periods need to be clearly specified and limited to what is absolutely necessary for the prescribed purpose.[50] While the Committee noted that masking out identifying data of the passenger after a certain time can mitigate certain risks of longer data retention, it recalled that masked out data still permits identification of the individuals concerned. Therefore, such data continues to be personal data, which must be subject to appropriate data retention limits in order to prevent permanent and general surveillance.[51] In the context of the COVID-19 pandemic, the collection of health data in addition to other already collected personal data may raise further human rights concerns for international travellers by air, and also by land and sea.

- Given the intrusiveness and large number of people affected by API and, especially, PNR, states **need to clearly and convincingly demonstrate how the use of this data is limited to what is strictly needed** to achieve a legitimate aim such as the prevention, detection or investigation of terrorist offences or other serious crimes.[52]
- To safeguard against excessive data collection, states need to **minimize the amount of data** that is being collected and **data retention periods,** as well as strictly observing **purpose limitations** for processing of data. Collection and processing of **sensitive data** as PNR should not be permitted.[53]

Accuracy, reliability and data-sharing across borders

Wrong or mismatched API or PNR data entries might impact an individual's right to freedom of movement and other rights. For example, if a person's name is misspelled in the API data, they could either be prevented from boarding the plane or from entering their country of destination. While API data is based on official travel documents, PNR data is entered manually by the traveller or the travel agent. The accuracy of PNR data is therefore not usually ascertained. Even with API data, errors may occur in data entry or handling. Discrepancies can generate suspicion and lead to travellers being wrongfully reported for suspected involvement in terrorism or other serious crime.[54]

49 In Canada, API and PNR data is kept for three-and-a-half years, unless there is an active investigation, in which case the data is kept for six years. For more information see, Canada Border Services Agency "Advance Passenger Information / Passenger Name Record Data", <https://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html>. In the United States, PNR data is retained for 15 years, the last 10 of which the data lays "dormant". For more information see: "How long is PNR information retained and what access restrictions apply?" under U.S. Customs and Border Protection "Passenger Name Record (PNR)", <https://www.cbp.gov/travel/clearing-cbp/passenger-name-record>. The EU Directive on PNR requires that data should be de-personalized after six months and that retention of the data must not exceed five years. However, the five-year retention period has been criticized as excessively long; and whether de-personalization provides for an effective safeguard for the protection of privacy rights has also been questioned because the data can be re-personalised.

50 See Council of Europe Consultative Committee of Convention 108, "Opinion on the Data protection implications of the processing of Passenger Name Records", Strasbourg, 19 August 2016, p. 8-9, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b051e>.

51 *Ibid.* This is consistent with decisions of the CJEU in other contexts, which do not allow "general and indiscriminate retention of data" for combatting crime or safeguarding national security, unless a serious threat of national security is present or foreseeable, it is subject to judicial or other independent scrutiny and only done temporarily. See CJEU "Press Release No 123/20", Luxembourg, 6 October 2020, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123en.pdf>.

52 See Council of Europe Consultative Committee of Convention 108, "*op. cit.*, note 50, p. 6.

53 *Ibid.*, p. 7 and 11.

54 *Ibid.*, p. 4.

Both API and PNR data are used to identify terrorist suspects among travellers through comparison with relevant watchlists and databases (see section on watchlists and alert systems below). Wrongful identification can impact freedom of movement. PNR data is also used for a general data analysis of the traveller, as well as specific risk assessments of behaviour to detect potential suspicious patterns. This can lead to discriminatory profiling, a risk that is further compounded if the aim of the data analysis is a predictive risk assessment. In that case, individuals may not only be identified as a risk on the basis of acts they might have committed but inferences about what they might do in the future.[55] This raises additional human rights concerns (see section on algorithmic decision making below).

Lack of adequate data protection standards and safeguards is an obstacle to information sharing between OSCE participating States. Sharing of PNR data across borders will only be lawful if the standards of privacy and data protection are safeguarded in both the sending and the receiving country.[56] But "only a few countries seem to have considered establishing effective mechanisms with this regard, including for redress."[57] Sharing data under such circumstances not only undermines data protection standards but could also result in other human rights violations (e.g., undue restrictions on freedom of movement, discrimination, unlawful detention or inhuman and degrading treatment or punishment) where human rights protections are inadequate in the receiving country. This could put not only the individual traveller at risk but also their families or associates. Sharing of this data can put refugees and asylum seekers at particular risk, if as a result they are prevented from leaving their or another country.

- In developing and implementing API and PNR systems, states need to put in place **effective human rights safeguards** to protect people from **being wrongfully placed under suspicion** for involvement in terrorism or other crime. In particular, states **must refrain from discriminatory profiling** on the basis of PNR data.
- Before entering into agreements for sharing of API and PNR data, states must ascertain that privacy and data protection, as well as other human rights safeguards, are fully in place and respected in partner countries with which such information is sought to be shared.

55 *Ibid.*, p. 8. See also UN Special Rapporteur on counter-terrorism, Intervention at the ODIHR Expert consultation meetings, 15 June 2020, <https://www.ohchr.org/Documents/Issues/Terrorism/SR/OSCEODIHRExpertMeetingAPI_PNRdata.pdf> and "Passenger Name Records, data mining & data protection: the need for strong safeguards", *op. cit.*, note 48.

56 See Council of Europe Consultative Committee of Convention 108, "*op. cit.*, note 50, p. 9, which recalls "that any PNR data transfers to States that are not Parties to Convention 108 must satisfy the conditions established to guarantee the appropriate protection of data subjects in such States".

57 OSCE Parliamentary Assembly, ad hoc Committee on Countering Terrorism "Strengthening Border Security and Information Sharing in the OSCE Region: A Parliamentary Oversight Exercise", October 2019, p. 11, <https://www.oscepa.org/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/3905-strengthening-border-security-and-information-sharing-in-the-osce-region/file>. Based on existing data protection standards, e.g., the EU PNR Directive states that data can only be shared with third-countries on a case-by-case basis in very limited circumstances. In 2017, the CJEU decided that the envisaged agreement between the EU and Canada regarding sharing of PNR data were incompatible with the right to privacy and protection. It found that the terms of the agreement for data retention, use and potential onwards transfer to Canadian, European or foreign public authorities unduly interfered with those rights as "several provisions of the agreement are not limited to what is strictly necessary" and that sensitive data was not adequately protected from being shared. As a result, the agreement could not be concluded. New negotiations were launched in 2018, but finalization of the agreement is still pending. So far agreements have been concluded with the United States and Australia. See CJEU "Press Release No 84/17", Luxembourg, 26 July 2017, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf>; and European Commission Report "On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime", Brussels, 24 July 2020, pp. 2-3, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-305-review_en.pdf>.

Biometric data systems

Biometrics are characteristics of a person that are individual and generally unchangeable, such as fingerprints, facial images, iris, voice, vascular patterns and DNA. These can be scanned or otherwise extracted and used to identify a person. Following its collection, biometric data is converted into numerical and standardised biometric templates. These templates are machine-readable and can be stored and compared with other biometric data.[58]

This comparison can either be with information stored in different databases (for example within travel permission IT systems) or with templates collected through so-called LiveCapture (for example at eGates).[59] Biometric data comparisons can either take the form of "verification" (verifying whether two biometric datasets originate from the same person), or "identification" (identifying whether the person's biometric data matches with an existing record in a specific database). Errors may occur in the form of "false acceptances" or "false rejections", i.e., the system incorrectly determines either that two biometric templates match or do not match with each other.[60]

Apart from using fingerprints and facial images for verification or authentication, which has become common, states are increasingly experimenting with new biometric systems to identify potential security threats at borders.[61]

> Biometric systems raise pressing human rights issues that include, but also go far beyond, implications for the right to privacy, especially for people in vulnerable situations such as migrants, refugees, asylum-seekers and children. **All systems that operate with biometric data should be presumed high-risk technologies:** accordingly they should undergo **thorough and independent human rights impact assessments.**[62]

58 For an overview of biometric systems and matching see, e.g., OSCE and Biometrics Institute "Outcome Document of the ID@ Borders & Future of Travel Conference 2019", 14 May 2019, <https://www.osce.org/secretariat/419552?download=true>.

59 LiveCapture is the process of collecting a biometric sample and converting it to a biometric template. However, the template is usually not stored in a database but immediately compared to different biometric templates, e.g., those stored on the chip of a biometric passport.

60 "UN Compendium", *op. cit.*, note 40, pp. 14 and 16.

61 E.g., in motion face recognition, gait recognition or even predictive biometrics, i.e. in addition to use of biometrics for verification or identification also use for predictive purposes. See Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?", 22 July 2020, p. 9, <https://www.ohchr.org/Documents/Issues/Terrorism/Use-Biometric-Data-Report.pdf>. On "technological experimentation" conducted by state and non-state actors on refugees, migrants, and stateless persons, see also UN Special Rapporteur on racism, *op. cit.*, note 18, paras 38-39; and "Technological Testing Grounds" *op. cit.*, note 19.

62 *Ibid.*, pp. 36 and 38. See also UN Special Rapporteur on racism, *op. cit.*, note 18.

Data protection principles

Biometric data is personal data, therefore, its collection, storage and processing constitute an interference with the right to privacy. Blanket and indiscriminate retention of biometric data has been found to be incompatible with the right to privacy.[63] Furthermore, biometric data is sensitive data[64] and it may also reveal other sensitive data, which requires special protection to avoid discrimination.[65]

In all cases the collection, storing and processing must be based in law, necessary and proportionate to achieve a legitimate aim.[66] However, in many countries the collection and processing of biometric data, in particular in the context of combatting terrorism and other crime, is still not sufficiently regulated in domestic legal frameworks.[67]

In many states, non-nationals entering the country are obliged to provide fingerprints and facial images at border crossings. In accordance with international data protection standards, everyone whose data is taken has a right of information about what data is collected, for which purpose, for how long it will be stored and how it is processed.[68] Therefore biometric data must not be collected covertly and stored.[69] When collecting and processing biometric data states have a duty to inform people of their rights as data subjects in a way that is understandable and accessible to them (for example through leaflets, illustrative materials and visible display at points where such data is collected).[70]

The Court of Justice of the European Union has held that taking and storing fingerprints in a passport chip is legally permissible as it does not imply any processing that would go beyond what is necessary to achieve the aim of protecting against the fraudulent use of passports.[71] This, however, only applies as long as the data is used for the intended purpose of verifying the authenticity of a passport and the identity of its holder as defined

---

63 European Court of Human Rights (ECtHR) "Marper v. The United Kingdom", Applications nos. 30562/04 and 30566/04, 4 December 2008, para 125, <https://rm.coe.int/168067d216> (with regards to fingerprints, cellular samples and DNA profiles).

64 See Council of Europe "Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", Article 8. The amending Protocol extends the specific categories of sensitive data to cover also biometric data in the modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called Council of Europe "Convention 108+"). Pending entry into force, states may declare to apply the amended rules of Convention 108+ on a provisional basis. The text of the modernized Convention 108+ is available at: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>. For the EU, the GDPR also refers to biometric data as sensitive data (Article 9, para 4). See also Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *op. cit.*, note 61, p. 16; and Privacy International "Responsible use and sharing of biometric data in counter-terrorism", July 2020, p. 8, <https://privacyinternational.org/sites/default/files/2020-07/Responsible%20use%20and%20sharing%20of%20biometric%20data%20in%20counter-terrorism.pdf>.

65 From certain biometric data also other information that qualifies as "special category of personal data" (sensitive data) can be inferred. E.g. DNA samples or voice or iris recognition tools can also provide information on the health, gender, age and ethnicity of a person. See Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *op. cit.*, note 61, p. 24.

66 See overview of case-law in ECtHR, "Factsheet – Personal data protection", October 2020, <https://www.echr.coe.int/Documents/FS_Data_ENG.pdf>.

67 According to Privacy International, approximately two-thirds of states worldwide have comprehensive data protection legislation in place. However, most of this legislation does not yet specifically cover biometric data. Furthermore, many of the laws contain exemptions for national security, combatting terrorism and crime. See Privacy International, *op. cit.*, note 64, p. 8.

68 Council of Europe "Convention 108", Article 8; and modernized "Convention 108+", Articles 8 and 9. EU General Data Protection Regulation (GDPR), Articles 13 and 14.

69 There may be exceptions to this rule, e.g., for the protection of national security and public order. See, e.g., the limitation clause under Article 9 of the Council of Europe "Convention 108" and Article 11 of the modernized "Convention 108+", respectively. However, in the PNR context, the Consultative Committee of Convention 108 recommended that persons who are not suspected of having committed, or being about to commit, a terrorist offence or other serious crime enjoy the full exercise of the right of information, access, correction and deletion. See Council of Europe Consultative Committee of Convention 108, "*op. cit.*, note 50, p. 9. In the EU, in collection and processing of personal data for law enforcement purposes the GDPR does not apply, but the Police Directive does.

70 For example in the EU; see EU Fundamental Rights Agency (FRA), "Under watchful eyes: biometrics, EU IT systems and fundamental rights", 2018, pp. 10 and 29-41, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf>.

71 CJEU, "Michael Schwarz v Stadt Bochum", Case C-291/12, Judgment of 17 October 2013, paras 63-64, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0291&from=EN>.

in the applicable law.[72] Undue interference with the right to privacy can arise when the data is used for other purposes or when the processing leads to storing in centralized fingerprint databases.[73] This appears to be the case where the data is used for "identification" (i.e., to screen the data against watchlists or alert systems) or if fingerprints taken at border controls for verification (e.g., at eGates during liveCapture), are not deleted immediately after verifying the identity of the traveller but are kept and stored.[74]

With the increasing development of large biometric databases, growing centralization of and interoperability between different databases,[75] there is ever more risk of what has been described as mission, purpose or function creep.[76] The mere availability of biometric data, or the possibility of easily obtaining it, leads to an expansion in its use.[77] This raises the risk of "re-purposing" of data sets for means other than the initial purpose for which the data was collected.[78] Moreover, greater interaction between law enforcement and immigration databases, which contributes to the portrayal of migration as a security threat, creates a risk of stigmatization of people in vulnerable situations, such as migrants, refugees and asylum-seekers, stateless persons, and persons living in precarious immigration status.[79]

72 *Ibid.*, para 56.

73 *Ibid.*, paras 61 and 62; European Data Protection Supervisor (EDPS) "EDPS Opinion 7/2018 on the Proposal for a Regulation strengthening the security of identity cards of Union citizens and other documents", 10 August 2018, para 42, <https://edps.europa.eu/sites/edp/files/publication/18-08-10_opinion_eid_en.pdf>. Regarding concerns about systematic storing of genetic data of everyone in immigration custody (i.e., to "warehouse the genetic data of people who have not been accused of any crime, for crime detection purposes", severing the longstanding prerequisite of prior alleged criminal conduct to compel DNA collection), see UN Special Rapporteur on racism, *op. cit.*, note 18, para 41.

74 Regarding non-EU citizens entering the Schengen area on the basis of a visa or an electronic travel approval, fingerprints and facial images will be stored in the Electronic Entry/Exit System (EES) when this will become operational in 2021. See, Statewatch "Automated Suspicion – The EU's New Travel Surveillance Initiatives", July 2020, p. 27, <https://www.statewatch.org/media/1235/sw-automated-suspicion-full.pdf>.

75 See Privacy International, *op. cit.*, note 64, p. 5. UN CTED, e.g., highlighted the need to compare biometric data, collected in border and immigration vetting and investigations, against wider national and international biometrics tools, for the identification of terrorists and recommended states to ensure interoperability of their biometric data systems with other national and international biometric databases. See UN CTED, "2018 Addendum to the 2015 Madrid Guiding Principles", UN Doc. S/2018/1177, December 2018, para 14 and Guiding Principle 3, <https://www.un.org/sc/ctc/wp-content/uploads/2018/12/2018-Addendum-to-the-2015-Madrid-Guiding-Principles_as_adopted.pdf>.

76 See Privacy International, *op. cit.*, note 64, pp. 14 and 16; Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *op. cit.*, note 61, pp. 24 and 28, and UN Special Rapporteur on racism, *op. cit.*, note 18, para 35.

77 See Privacy International, *op. cit.*, note 64, p. 14.

78 *Ibid.* Co-optation of data sets for other means has been documented in population monitoring of refugees and the subsequent use of data for COVID-19 modelling. See Crofton Black, "Monitoring being pitched to fight Covid-19 was tested on refugees", 28 April 2020, <https://www.thebureauinvestigates.com/stories/2020-04-28/monitoring-being-pitched-to-fight-covid-19-was-first-tested-on-refugees>.

79 See Privacy International, *op. cit.*, note 64, p. 14-15 with reference, e.g., to EURODAC, which was established in 2004 to facilitate application of the Dublin Regulation and is also being used since 2009 for law enforcement purposes, especially to counter terrorism, as noted by the EDPS. With reference to the involvement of private companies and the push towards interoperability between law enforcement and immigration databases also see UN Working Group on the use of mercenaries, *op. cit.*, note 18, para 40; as well as Statewatch and PICUM, "Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status", 18 November 2019, <https://www.statewatch.org/media/documents/analyses/Data-Protection-Immigration-Enforcement-and-Fundamental-Rights-Full-Report-EN.pdf>.

- States must put in place clear **human rights-based frameworks,**[80] which reflect the nature of **biometrics as sensitive data** and strictly regulate the use of biometric technology.
- The framework must provide limits to the expanding use of biometrics and increasing **centralization and interoperability**, and afford effective **protection against re-purposing** and **covert collection** of biometric data (right to information).When collecting and processing biometric data, this must be **provided by law, strictly necessary, proportionate and non-discriminatory**.
- Particular care must be taken to avoid stigmatization of groups in situations of particular vulnerability such as refugees, asylum-seekers and persons living with a precarious immigration status.

Biometric data, vulnerability and dignity

Refugees, asylum-seekers and children crossing borders are at particular risk of human rights violations arising out of the use of biometric data. In addition to privacy and data protection concerns, there are particular risks of infringements of absolute rights, including the risk of refoulement, cruel, inhuman and degrading treatment, or other infringements on human dignity. These risks not only relate to the storage and use of biometric data, but also the way it is collected.

States commonly require the collection of fingerprints and facial images for asylum applications.[81] As pointed out by the UN Special Rapporteur on racism, particularly data collection, "in contexts characterized by steep power differentials, raise[s] issues of informed consent and the ability to opt out."[82] Where giving fingerprints is a pre-requisite for applying for asylum, as in for example the EU, the refusal might lead in practice to inability to seek refuge.[83] In some states, it can also lead to detention or other coercive measures for taking of fingerprints.[84] Reports of incidents involving the use of force, which allegedly amounted to cruel, inhuman or degrading treatment have been documented in some countries.[85]

Fleeing from persecution, refugees and asylum-seekers are in stressful situations already, especially when transiting through dangerous routes and arriving in often hostile environments. This is amplified by coercion in the collection of biometric data and if they are not informed properly about why their fingerprints are taken, where they will be stored and how they could access, correct or have them deleted.[86] There is a risk that children or other vulnerable groups, including victims of trafficking and individuals who have experienced gender-based violence, may not give free and informed consent. People may also refuse to give fingerprints where they fear that data may be shared with their country of origin.[87] The UN High Commissioner for Refugees has highlighted the danger of sharing data of asylum-seekers with their countries of origin; people may be subjected to reprisals upon return or their family members may face persecution while remaining in the country.[88] While this applies to

80 As also recognized by UN CTED, "2018 Addendum to Madrid Guiding Principles", *op. cit.*, note 75, Guiding Principle 3, para (d).
81 For example in the EU; see FRA "Under watchful eyes", *op. cit.*, note 70.
82 UN Special Rapporteur on racism, *op. cit.*, note 18, para 34.
83 See "Under watchful eyes", *op. cit.*, note 70, p. 51.
84 *Ibid.*, pp. 53 and 55-56.
85 *Ibid.*, pp. 53-54.
86 For examples, see "Technological Testing Grounds", *op. cit.*, note 19, pp. 12-14
87 See FRA "Under watchful eyes", *op. cit.*, note 70, pp. 10, 49 and 77-79.
88 The UN High Commissioner for Refugees (UNHCR) "Addressing Security Concerns without Undermining Refugee Protection - UNHCR's perspective", 17 December 2015, para 17, <https://www.refworld.org/docid/5672aed34.html>; and "Under watchful eyes", *op. cit.*, note 70, pp. 77-78.

all types of data, there appear to be heightened risks for biometric data due to its greater potential to be used for further exclusion, discrimination and state surveillance in the country of origin.[89]

The increased use of biometrics has also resulted in people's bodies becoming a form of identification. This may threaten their physical integrity. For example, people may resort to self-harm if they are afraid of the risks associated with being identified.[90] Risks of "identity theft" can also create long term problems since the biometrics of individuals cannot be replaced if the biometrics of an individual is hacked.

The COVID-19 pandemic, the subsequent increased collection of data and the appetite for technological responses has raised concern due to its possibly far reaching effects on human rights and civil liberties. Data collected for the purposes of the containment of COVID-19 may be used to further infringe on people's rights, particularly when used in combination with biometric data and in settings with high human rights risks, for example, for marginalized people on the move.[91]

- In particular for people in **situations of heightened vulnerability**, including migrants and asylum-seekers, states must ensure that the principle of **free and informed consent,** as well as the **right to information,** are guaranteed in practice in connection with the collection and processing of biometric data such as fingerprints.
- Under no circumstances may the collection and use of biometric data result in restrictions of absolute rights. **Human dignity, prohibition of cruel, inhuman or degrading treatment** and ***non-refoulement*** must be fully respected at all times.
- States should follow the well-established principle **not to share the biometric data of asylum seekers with the country of origin**.[92]

Reliability and discriminatory bias

While biometric data is often perceived as unchangeable, it does change over time as our bodies change. The quality of fingerprints for example decreases with age, skin diseases or hard manual labour. Facial recognition systems operating on the basis of biometric data have been described as inherently fallible since they inevitably rely on statistical probabilities.[93]

The levels of inaccuracy in biometric face recognition algorithms depend heavily on gender, skin colour and age. Studies have shown that existing face recognition algorithms had more difficulties to recognise female faces and produced more false rejections and false acceptances for female faces. They also produced more

89 See, e.g., The Institute of Statelessness and Inclusion "Locked in and locked out: The impact of digital identity systems on Rohingya populations", November 2020, p. 3, <https://files.institutesi.org/Locked_In_Locked_Out_The_Rohingya_Briefing_Paper.pdf>.

90 See, "Under watchful eyes", *op. cit.*, note 70, pp. 50 and 56; and "Technological Testing Grounds", *op. cit.*, note 19, pp. 12-14, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf>.

91 "Technological Testing Grounds", *op. cit.*, note 19, pp. 21-22.

92 UNHCR "Addressing Security Concerns without Undermining Refugee Protection", *op. cit.*, note 88 para 17.

93 Sandra Azria and Frédéric Wickert "Facial Recognition: Current Situation and Challenges", Study prepared for the Consultative Committee for Convention 108, Strasbourg, 13 November 2019, pp. 15-16, <https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1>.

accurate results for lighter faces than dark ones and had the highest error rate on darker female faces.[94] This can lead to intersectional discrimination of black women, for example, as results based on their biometric data are most prone to error.[95]

Inaccurate results of biometric systems due to gender, skin colour, ethnicity or other protected characteristics may have a discriminatory impact and other serious consequences for travellers. Both mismatches and false positives – for example in facial recognition at eGates or fingerprint scans – can be stigmatizing, reinforce negative stereotypes and lead to people being placed wrongly under suspicion. They can result in more detailed inspections or other disadvantages at border crossings or even prevent travel.[96] While subsequent human checks may in principle correct machine errors, the tendency to trust technology more than other information and human judgement (so-called "automation bias") may inhibit this and reinforce discriminatory bias.[97]

There is also an increasing tendency to develop predictive tools, such as automated deception or emotion detection, scans for facial expressions, or voice analysis based on biometric data. This trend greatly exacerbates the human rights risks.[98] Such technologies are not sufficiently reliable or accurate. But aside from the question of error, the use of biometric data to analyse an individual's emotional or mental state or, for example, to predict criminality raises serious concerns, including about the right to freedom of thought and the right to mental integrity.[99]

---

94 Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" Proceedings of Machine Learning Research 81:1–15, 2018 Conference on Fairness, Accountability, and Transparency, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>. See also Patrick Grother, Mei Ngan and Kayee Hanaoka for the National Institute of Standards and Technology (NIST) U.S. Department of Commerce "NISTIR 8280 Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", December 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

95 In the past, face recognition algorithms have also shown to best recognize the faces that are most common in the region where the systems have been developed. E.g., facial recognition algorithms from East Asia performed best on Asians and algorithms developed in the Western hemisphere performed best on lighter skin faces. However, more recent studies suggest that training of such algorithms with more diverse data sets may improve system accuracy. See Patrick Grother, Mei Ngan and Kayee Hanaoka, *op. cit.*, note 94. For more general information on the relationship between machine bias and systemic racism, see also Ruha Benjamin, "Race After Technology: Abolitionist Tools for the New Jim Code", 2019.

96 For asylum-seekers false biometric outputs can lead to them being banned from entering the country of asylum, wrong Dublin transfers in the case of the EU, wrongful detention or, in case of refoulement, even put them at risk of torture and other ill-treatment or other serious human rights violations.

97 For more on "automation-bias" see also next section and Petra Molnar "Technology on the margins: AI and global migration management from a human rights perspective", 2019, Cambridge Journal of International Law, Vol. 8. No.2, p. 324.

98 See UN Special Rapporteur on racism, *op. cit.*, note 18, para 39, with reference to iBorderCtrl, an EU project piloted at the borders of a number of EU member states. See also Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *op. cit.*, note 61, p. 25.

99 Guaranteed by Article 18 of the ICCPR and Article 3 of the EU Charter of Fundamental Rights, respectively. For concerns about the lack of accuracy of such systems see e.g. Ryan Gallagher and Ludovica Jona, "We tested Europe's new lie detector for travelers — and immediately triggered a false positive", The Intercept, 26 July 2019, <https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector/>; and Samuel Stolton, "MEP: Public has a 'right to know' about Commission's lie detector tech", EURACTIV, 1 April 2020, <https://www.euractiv.com/section/digital/news/mep-public-has-a-right-to-know-about-commissions-lie-detector-tech/>. For concerns about the use of predictive technology in policing see, e.g., PACE, Resolution 2342 "Justice by algorithm – The role of artificial intelligence in policing and criminal justice systems", 22 October 2020, <https://pace.coe.int/en/files/28805/htm>.

- States should reconsider the use of biometric technology, such as facial recognition, which may **reinforce bias and result in discrimination**.
- They should refrain from deployment and operation of **untested or inaccurate technological tools,** in particular in areas such as border management or migration which already in themselves bring high human rights risks for those affected.
- Where, after thorough impact assessment, the deployment and use of biometric technology is found appropriate, states need to ensure that **potential human rights risks are mitigated**, including by addressing **automation bias** and providing procedural safeguards and training.

Algorithmic decision-making in visa, travel authorization and screening systems

Algorithms are systems that are programmed to analyse data statistically and make predictions, recommendations or to inform decisions according to a set of rules.[100] While algorithmic or automated decision-making systems are designed by humans, they can be trained to change and adapt automatically over time in response to different data sets. In practice, this means that algorithms may learn to assign certain properties to particular characteristics.[101] For example, an algorithm could learn from a certain collection of data sets that everyone over a certain height is male so that it later automatically identifies all taller people as men. Such machine-learning and changes to the system can take place with varying degrees of autonomy or supervision.[102]

Applied to border management, recommendations or predictions made by algorithms are sometimes used to help decide whether an individual is allowed to travel or to enter a country,[103] whether to submit someone to further screening or checks or to determine whether a person represents a threat. In the case of visa request or travel approval systems, the personal data of the traveller is analysed to assist in making a determination whether to approve or deny the travel request.[104] Similarly, personal data is analysed for indicators of a perceived threat in screening and risk assessment for counter-terrorism or other purposes in border control.[105] Algorithms can therefore have a huge impact on individual rights in the context of border management.

---

100 FRA, "#BigData: Discrimination in data-supported decision making", 2018, pp. 3-4, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-focus-big-data_en.pdf>, and on different meanings of the term "algorithm" in formal mathematics and computer science definitions and its popular usage in public discourse Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi, "The ethics of algorithms: Mapping the debate", Big Data & Society, December 2016, pp. 2-4, <https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679>.

101 *Ibid.*, "The ethics of algorithms", pp. 2-4.

102 For different concepts of machine learning, artificial intelligence and the distinction between supervised and unsupervised learning see *Ibid.*, p. 3; Privacy International "Submission on Draft General Recommendation No. 36: Preventing and Combating Racial Profiling", June 2019, pp. 2-4, <https://privacyinternational.org/sites/default/files/2019-07/PI%20submission_CERD%20General%20Comment%2036_June%202019.pdf>; and Council of Europe Commissioner for Human Rights "Unboxing Artificial Intelligence: 10 steps to protect Human Rights", 2019, p. 24, <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>. Both, the documents of Privacy International and the Council of Europe Commissioner for Human Rights, contain a useful glossary of related terms and concepts.

103 A growing number of countries are using electronic visa application systems. For visa exempt travel, a number of countries also use electronic travel authorization systems, such as ESTA in the United States and eTA in Canada. The EU is setting up a similar system, so-called ETIAS, which is expected to be operational in 2022.

104 This data may include but is not limited to personal data (i.e., name, date and place of birth, gender, profession), a series of questions (purpose of travel, duration of travel, possible past criminal offenses), biometric data and information about travel companions. For a comparison of data required in different countries, see Tactical Tech, "Applying for a Visa", <https://ourdataourselves.tacticaltech.org/posts/40-applying-for-a-visa>.

105 This may also include PNR data, which is analyzed by so-called passenger information units (PIUs) for detection of "terrorist travel" prior to border crossing.

Algorithmic bias and automation bias

Also in the border context, algorithms are often seen as neutral technical tools that help to screen individuals and inform consequent decision-making, for example on whether to allow entry, based on correlations and patterns in objective data. However, technology is not neutral to the extent that there is a risk of introducing bias to the algorithm through biased data sets, which will be replicated in the analysis of the data and then influence the final decision.[106]

To avoid wrongful identification of travellers as suspects or persons posing terrorism-related threats, the Consultative Committee of Convention 108 underlined that the relevance of individual results of automatic assessments should be carefully examined by a person in a non-automated manner.[107] Officers conducting such examination must be adequately trained and sensitized to potential bias and the implications of erroneous risk identification for the people concerned.[108] However, the issue of automation bias, or the predisposition of human decision-makers to assume that decisions rendered by technology are more neutral and objective than decisions made by humans, introduces additional problems that are difficult to identify, let alone to correct.

Algorithms can also produce self-reinforcing bias. With the dynamic advancement of the algorithm through (autonomous) machine learning the bias becomes increasingly difficult, or even impossible, to trace and to correct. If an algorithm is advanced through a "training set", "it creates a significant risk of involuntarily reproducing existing prejudices and of perpetuating social inequalities and the stigmatisation of certain groups."[109] For example, if a visa algorithm is given data that is biased against certain nationalities, this can lead to the algorithm "learning" from that data that travellers from these countries are less likely to have their visa application approved, which will in turn reinforce the initial bias.[110] Where self-reinforcing bias reproduces itself, it is difficult to mitigate since it might not be clear why the algorithm has come to certain conclusions. Where it results in arbitrary denial of visa or travel authorization, it is not only discriminatory but can also impact travellers' freedom of movement and other rights such as the right to family life.

106 "#BigData: Discrimination in data-supported decision making", 2018, *op. cit.*, note 100, p. 5.

107 See Council of Europe Consultative Committee of Convention 108, *op. cit.*, note 50, p. 8. This is also required by the EU PNR Directive, *op. cit.*, note 57.

108 In addition, those concerned should have access to effective remedies and a right to information and rectification of their data etc. See Council of Europe Consultative Committee of Convention 108, *op. cit.*, note 50, pp. 9-10. This is also recognized by the UN CTED, "2018 Addendum to Madrid Guiding Principles", *op. cit.*, note 75, pp. 6-7.

109 FRA "Preventing unlawful profiling today and in the future: a guide", 2018, p. 110, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf>.

110 See, e.g., "Home Office drops 'racist' algorithm from visa decisions", BBC News, 4 August 2020, <https://www.bbc.co.uk/news/technology-53650758>; and Henry McDonald "AI system for granting UK visas is biased, rights groups claim", The Guardian, 29 October 2019, <https://www.theguardian.com/uk-news/2019/oct/29/ai-system-for-granting-uk-visas-is-biased-rights-groups-claim>.

- Algorithmic/automated decision-making tools must always remain under **human control**[111] and be **transparent**. Results of assessments that put individuals at a disadvantage must be carefully examined in a non-automated manner.
- Algorithmic systems should undergo **obligatory audit and "discrimination testing,"** prior to deployment and regularly thereafter, as well as an assessment of how the selection of data-sets, their processing, decision-making modalities and outputs impact human rights.
- States should extend obligations to conduct such assessments to **private companies as well as public bodies** involved in the development and operation of such systems. Assessments must incorporate **independent human rights expertise** and be **transparent and participatory**, involving relevant national institutions[112] as well as non-governmental organizations reflecting the diversity of society, as well as groups and communities whose rights are most affected.
- Border guards and others involved in the development and operation of algorithmic systems should receive appropriate **human rights and anti-discrimination training**. Users should be trained to understand risks and limitations of the systems and recognize **personal biases and "automation bias."**

Risk assessment and discriminatory profiling

The inherent risk of bias in the design of algorithms and the data they are trained on may lead to discriminatory profiling.[113] Categorizing individuals on the basis of assumptions about certain groups, or perceived patterns they are presumed to be associated with, may stigmatize people by attaching a specific risk profile to them and reinforce stereotypes about entire groups or communities. As a result, such profiling reinforces discrimination against members of those groups or communities.[114] Identifying certain characteristics of people as a "risk pattern," may constitute discriminatory profiling, especially if these risk patterns involve protected characteristics, such as ethnicity, colour, gender, language, religion, political or other opinion, national or social origin or other status. Discriminatory profiling is unlawful.

A combination of personal information about a person, which is used in visa and travel authorization systems, may also reveal protected characteristics. For instance, from information about the level of education and current occupation required for the new European Travel Information and Authorisation System (ETIAS), conclusions could be drawn about religion if the person has attended religious education and/or worked in religious institutions.[115] If such conclusions are used in algorithmic risk assessment or screening and result in individuals being singled out as a potential security risk, it may constitute discriminatory profiling and can impact their freedom of movement and other human rights.

---

111 "Unboxing Artificial Intelligence", *op. cit.*, note 102, p. 13.

112 Such as National Human Rights Institutions (NHRIs), data protection and equality bodies.

113 For the purpose of this policy brief, profiling is defined as making assumptions about the behaviour of a person based on their characteristics and/or previous behaviour. See FRA "Towards More Effective Policing – Understanding and Preventing Discriminatory Ethnic Profiling: A Guide", 2010, pp. 9-10, <https://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf>.

114 *Ibid.* See also Council of Europe Commissioner for Human Rights, "Ethnic profiling: a persisting practice in Europe", 9 May 2019, <https://www.coe.int/en/web/commissioner/-/ethnic-profiling-a-persisting-practice-in-europe>; and CERD, General recommendation No. 36, *op. cit.*, note 29.

115 FRA "The impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS) Opinion of the European Union Agency for Fundamental Rights", Vienna, 30 June 2017, pp. 19, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-opinion-02-2017-etias.pdf>.

Categorizing individuals and assigning risk profiles due to a particular combination of characteristics can be misleading. For example, travellers from a specific country/region who work in low-skilled professions might be seen as displaying patterns of characteristics associated with irregular migration, but the travel pattern and individual characteristics might also be typical for their country/region. Even if the risk categorization is not based on protected characteristics, discrimination can occur inadvertently if it affects certain groups disproportionately or indirectly.[116] People criminalized on account of their sexual orientation in their countries of origin will likely face further discrimination when travelling if an algorithm does not know how to differentiate between different "past criminal offenses."[117] The use of algorithms to identify characteristics like sexual orientation should never be allowed.

Generally, association with a certain risk profile may have serious human rights implications for the individuals concerned, for example if, as a result, they are prevented from leaving a country or refused entry, subjected to further screening and security checks in a discriminatory manner or even detained when attempting to cross a border. In the case of asylum seekers, such an association could expose them to torture and other cruel, inhuman or degrading treatment or a risk to their life if returned to or prevented from leaving their country.[118]

- In algorithmic analysis of travel data for screening and risk assessment, states must **refrain from discriminatory profiling at all times**.[119]
- In order to prevent discrimination and discriminatory profiling effectively, states need to establish **clear legal and human rights-based frameworks** that strictly regulate the development and operation of algorithmic risk assessment tools and **the way in which individual results are used or potentially shared**.
- The regulatory framework has to include **human rights safeguards** to protect data-subjects, including the **right to information** about how their data is collected and for what purpose, as well as **effective remedies** to challenge it and any decisions based on the data generated from these systems.
- The operation of algorithmic systems must be subject to **effective and independent oversight** at all stages.

116 For example, if members of certain ethnic groups are overrepresented among people of low education level in a particular country and the latter is defined as a risk profile for irregular migration. *Ibid.*, pp. 28-29.

117 FRA "Preventing unlawful profiling", *op. cit.*, note 109, pp. 117-118; and FRA Opinion on the ETIAS Regulation, *op. cit.*, note 115, p. 21.

118 Petra Molnar and Lex Gill "Bots at the Gate - A Human Rights Analysis of Automated Decision-making in Canada's immigration and refugee system", 2018, <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>.

119 This is also recognized by UNSC Resolution 2396 (2017), para 4; and UN CTED, "2018 Addendum to Madrid Guiding Principles", *op. cit.*, note 75, Guiding Principle 1, para (d).

Watchlists and alert systems

There are many different information systems that are employed in border security measures for different purposes.[120] Watchlists or other databases of "known and suspected terrorists", as foreseen under UN Security Council Resolution 2396 (2017), are law enforcement alert systems. They are used "to screen travelers and conduct risk assessments and investigations."[121]

While access to watchlists and law enforcement databases is shared domestically between relevant law enforcement and border control authorities, Resolution 2396 also encourages states to share this information through bilateral and multilateral mechanisms. Multilateral mechanisms may include regional or international alert systems, such as those operated by Interpol. Based on information provided by national police forces, Interpol issues different types of notices about wanted and other individuals.[122] In the border security context, travel-related data such as API, PNR and information from travel approval or visa information systems, are checked against such national or international watchlists or law enforcement databases in order to detect wanted persons, suspects or individuals who are considered to pose terrorism or other crime-related threats.[123]

UNSC Resolution 2396 highlights effective implementation of enhanced screening mechanisms and international co-operation for information sharing as key for detection of "known and suspected terrorists" and stopping terrorist travel.[124] But terrorism watchlists are also **prone to misuse, which presents profound human rights and rule of law challenges** that states need to address in the implementation of the resolution.[125]

120 For an overview of the various IT information systems for sharing information relevant to security, migration and external border management, in the European Union see "EU Information Systems – Security and Border", European Commission, February 2019, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190205_security-union-eu-information-systems_en.pdf>.

121 UNSC Resolution 2396, United Nations Security Council, adopted 21 December 2017, paras 13 and 15, <https://ndocs.org/en/S/RES/2396(2017)>.

122 Interpol issues so-called "red notices" primarily for arrest of wanted persons or "blue notices" to collect additional information about a person's identity, location or activities in relation to a crime. See "About Notices", Interpol, <https://www.interpol.int/en/How-we-work/Notices/About-Notices>. In addition to notices, Interpol also maintains various databases on forensics (crime-related biometrics), lost and stolen passports, etc. See "Our 18 Databases", Interpol, <https://www.interpol.int/en/How-we-work/Databases/Our-18-databases>.

123 In ETIAS, the EU travel authorization system currently being set up, applications will be checked automatically against a number of EU security, migration and border management databases, as well as Interpol and Europol data. In addition, ETIAS will also include a watchlist. See Council of the EU, "European travel information and authorisation system (ETIAS): Council Presidency and European Parliament provisionally agree on rules for accessing relevant databases", Press Release, 18 March 2021, <https://www.consilium.europa.eu/en/press/press-releases/2021/03/18/european-travel-information-and-authorisation-system-etias-council-presidency-and-european-parliament-provisionally-agree-on-rules-for-accessing-relevant-databases>.

124 See e.g., Global Counterterrorism Forum (GCTF) "New York Memorandum on Good Practices for Interdicting Terrorist Travel", 25 September 2019, p. 1, <https://toolkit.thegctf.org/Portals/1/Documents/En/New_York_Memorandum_on_Good_Practices_for_Interdicting_Terrorist_Travel.pdf>.

125 As also recognized by the Addendum to the Madrid Guiding principles, para 11. See UN CTED, "2018 Addendum to Madrid Guiding Principles", *op. cit.*, note 75, para 11.

Overbroad listing criteria and arbitrary application

Wrongful inclusion in terrorism watchlists has serious human rights implications for the individual concerned.[126] Depending on the specific measures triggered by an alert from a watchlist (e.g., a travel ban, denial of entry or stay, questioning, surveillance or even arrest) it may impact a broad range of rights, including freedom of movement, access to international protection, privacy, the right to liberty, a fair trial and due process rights. It can also directly or indirectly affect the full spectrum of civil, political, economic, social and cultural rights of family members, including children, and associates of those listed.[127]

There is a risk of overbroad listing criteria and arbitrary inclusion on lists. This is partly due to the lack of a universally agreed definition of terrorism at the international level; overbroad definitions in national counter terrorism laws are prone to excessive or even abusive application.[128]

The emphasis of Resolution 2396 on "known or suspected terrorists," also raises questions as to the evidentiary thresholds for inclusion on the list and concerns around the presumption of innocence.[129] Particular concerns have been expressed about "pre-crime" watchlists that include "potential" terrorists or criminals, i.e., people who have not committed an offence but who may supposedly commit a crime in the future.[130] Inclusion on a terrorism watchlist, which comes with potentially far-reaching human rights restrictions, cannot be based on an abstract or hypothetical danger that a crime may happen in the future. For it to be necessary and proportionate, it must be linked to, "an actual, distinct and measurable terrorism threat,"[131] and there must be sufficient evidence of involvement in an actual criminal offence.

To avoid overbroad application of terrorism watchlists, **the criteria for including individuals on such lists must be clearly defined based on a narrow and precise definition of terrorist offences**.[132]

126 See e.g., ECtHR "Nada v Switzerland", Application no. 10593/08, 12 September 2012, <http://hudoc.echr.coe.int/fre?i=001-113118>; CCPR "Sayadi and Vinck vs Belgium", UN Doc. CCPR/C/94/D/1472/2006, 22 October 2008, <https://juris.ohchr.org/Search/Details/1477>. See also, Guidelines for Addressing the Threats and Challenges of 'Foreign Terrorist Fighters' within a Human Rights Framework, *op. cit.*, note 5, pp. 22-23.

127 The UN Special Rapporteur on counter-terrorism underlined that listing of children should generally be avoided. See UN Special Rapporteur on counter-terrorism, "Human Rights Principles Applicable to Watchlisting", 2020, Principle 9, <https://www.ohchr.org/Documents/Issues/Terrorism/ApplicablWatchlisting.docx>.

128 See e.g., UN Special Rapporteur on counter-terrorism "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders", 1 March 2019, UN Doc. A/HRC/40/52, <https://undocs.org/A/HRC/40/52>; or ODIHR, "The Responsibility of States': Protection of Human Rights Defenders in the OSCE Region (2014–2016)", 14 September 2017, <https://www.osce.org/odihr/341366>.

129 If "known terrorist" refers to persons convicted for a terrorist offence in a court, it requires proof of guilt beyond reasonable doubt; thresholds for different levels of suspicion (for prosecution, to order an arrest or initiate an investigation) are inevitably lower.

130 "Automated Suspicion – The EU's New Travel Surveillance Initiatives", *op. cit.*, note 74, pp. 22 and 33, with reference to the new ETIAS watchlist, which will be introduced in 2021 and will contain data on people suspected of having committed crimes in the past, as well as those who it is believed may commit crimes in the future.

131 As the UN Special Rapporteur on counter-terrorism highlighted in "Human Rights Principles Applicable to Watchlisting", *op. cit.*, note 127, Principle 2.

132 ODIHR consistently calls for counter-terrorism legislation to be based on a definition of terrorism that follows the approach of UNSC Resolution 1566 (2004); see e.g., ODIHR "Guidelines for Addressing the Threats and Challenges of 'Foreign Terrorist Fighters' within a Human Rights Framework", *op. cit.*, note 5, pp. 21-24. For a proposed model definition of terrorism based on those criteria see UN Special Rapporteur on counter-terrorism, "Ten areas of best practices in countering terrorism", 22 December 2010, UN Doc. A/HRC/16/51, para 28, <https://undocs.org/A/HRC/16/51>. On the definition of terrorism see also: ODIHR "Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community Policing Approach", February 2014, pp. 27-30, <https://www.osce.org/files/f/documents/1/d/111438.pdf>.

Lack of procedural safeguards in listing and delisting

Although improvements have been made over the past years, even the listing practice of international institutions, such as the UN Security Council and the European Union, have faced strong criticism.[133] Minimum due process standards must apply to all terrorism listing and sanctions regimes, both national and international. These include the requirement that individuals (or entities) are promptly informed of their placement on the list and the reasons for it; and have a right to apply for delisting and to court review of decisions resulting from such applications with full due process guarantees, including disclosure of relevant case information to the applicant.[134]

In practice, de-listing has proved particularly difficult if watchlists or database entries are shared transnationally. Even if an individual successfully challenges inclusion on the list in one country, this does not necessarily lead to delisting in all other countries. Separate applications and legal proceedings in different jurisdictions may be needed, which undermines the right to effective remedy.[135] Delisting in one jurisdiction should therefore also trigger a re-assessment of the listing in others, with effective access for those affected to legally challenge continued listing in other jurisdictions.[136] The use of sunset clauses, so that the listing automatically lapses unless renewed, has also been recommended.[137]

Due to far reaching human rights implications for individuals placed on a list, **stringent procedural safeguards** must be in place to protect against arbitrariness, in particular **effective remedies** to challenge wrongful listing, as well as **effective measures to secure delisting in practice**, also when watchlists or data are shared transnationally.

Privacy and data protection concerns

Screening of ordinary traveller data to detect suspected terrorists (and other criminal suspects) is not only done against national and international terrorism sanctions lists. It is also checked against various other law enforcement databases, which contain data of large numbers of people fed into the system by a broad range of different actors (police, intelligence, border authorities, etc.), without data subjects necessarily becoming

133 See e.g., PACE, Resolution 1597 "United Nations Security Council and European Union blacklists", 23 January 2008, <https://pace.coe.int/en/files/17618/html. In response to such concerns, the UN Security Council established an independent Office of Ombudsperson to review requests from individuals and groups seeking to be removed from the UN's sanctions list. See United Nations Security Council "Ombudsperson to the ISIL (Da'esh) and Al-Qaida Sanctions Committee", <https://www.un.org/securitycouncil/ombudsperson>.

134 These recommendations were made by the UN Special Rapporteur on counter-terrorism already in 2010, see "Ten areas of best practices in countering terrorism", *op. cit.*, note 132, practice 9. See also UN Special Rapporteur on counter-terrorism, "Human Rights Principles Applicable to Watchlisting", *op. cit.*, note 127, Principle 7.

135 The same applies when watchlists are reproduced and shared by private actors, e.g. for use by airlines or financial institutions, to ensure compliance with UNSC sanctions lists. As a result, individuals may experience ongoing restrictions, e.g., in opening bank accounts, even after delisting. See Gavin Sullivan, Submission to the UN Special Rapporteur on counter-terrorism, 2019, <https://www.ohchr.org/Documents/Issues/Terrorism/SR/Submissions/Gavin%20Sullivan_GA74CT.pdf>.

136 UN Special Rapporteur on counter-terrorism, "Human Rights Principles Applicable to Watchlisting", *op. cit.*, note 127, Principle 8. Similar recommendations have been made by PACE, i.e. to ensure that all copies of red notices or diffusions that have been found to be unjustified by Interpol must be deleted from national databases. See PACE Resolution 2315 "Interpol reform and extradition proceedings: building trust by fighting abuse", 29 November 2019, <https://pace.coe.int/en/files/28303/html>.

137 The UN Special Rapporteur on counter-terrorism recommended a sunset clause of 12 months, see "Ten areas of best practices in countering terrorism", *op. cit.*, note 132, practice 9.

aware of their inclusion in the database.[138] Under such circumstances oversight is difficult; and effective remedies, the possibility to challenge wrongful inclusion and request rectification are seriously hampered.

While broad exemptions from data protection laws are frequently applied to law enforcement, any interference with the right to privacy must be prescribed by law, necessary and proportionate to meet a legitimate aim.[139] Accordingly, the creation and maintenance of law enforcement databases must be based on legislation that provides for effective safeguards against abuse,[140] including time limits for data retention and particular protection of sensitive data such as information on someone's political views,[141] and the real possibility of requesting deletion of data[142] and rectification of false data.[143]

- Given the profound human rights impact of watchlists and other law enforcement databases, it is essential that appropriate procedures are in place to **review data regularly** to ensure it remains correct and that information that is no longer relevant and up-to-date is deleted in accordance with clearly **specified retention periods**.[144]
- Furthermore, the **possibility for data subjects to request rectification** must be effective and particular protections of **sensitive data** must be in place.

International co-operation

The sharing of watchlists and other databases in international law enforcement co-operation, whether bilateral or multilateral, further exacerbates potential human rights risks.[145] Collecting, sharing and receiving information from states where there is a real risk that this information has been obtained by torture or other ill-treatment make the receiving state complicit in such acts.[146] The same could be said about receiving data that was obtained through other serious human rights violations in the sending state. Similarly, sending information

138 In the EU, apart from the EU terrorism sanctions list, e.g., also the Schengen Information System (SIS) and Europol databases. A data entry in SIS may contain different instructions for the users of the system. Apart from arrest or refusal of entry of the person concerned, the system may also instruct the officers to conduct discrete or specific checks. In case of discrete checks the individual will not be aware that they are subject of an alert. See, "Automated Suspicion – The EU's New Travel Surveillance Initiatives", *op. cit.*, note 74, p. 22. For concerns regarding secretive terrorism/no fly lists see also American Civil Liberties Union (ACLU) "Wilwal v. Bielsen – Lawsuit challenging abusive border detention of American family", 29 September 2020, <https://www.aclu.org/cases/wilwal-v-nielsen-lawsuit-challenging-abusive-border-detention-american-family>; ACLU "Kashem, et al. v. Barr, et al. – ACLU challenge to Government No Fly List", 13 March 2018, https://www.aclu.org/cases/kashem-et-al-v-barr-et-al-aclu-challenge-government-no-fly-list and ACLU "Trapped in a Black Box: Growing Terrorism Watchlisting in Everyday Policing", April 2016, <https://www.aclu.org/sites/default/files/field_document/wirac_9-11_clinic_trapped_in_a_black_box.pdf>.

139 E.g., in the EU, law enforcement is explicitly not subject to data protection regulations of the GDPR but governed by the EU law enforcement directive (2016/680). Also in national data protection rules there are often broad exemptions for law enforcement. See section on biometrics. However, international data protection standards should be fully observed also in watchlisting as the UN Special Rapporteur on counter-terrorism highlighted; see UN Special Rapporteur on counter-terrorism, "Human Rights Principles Applicable to Watchlisting", *op. cit.*, note 127, Principle 6.

140 See e.g., ECtHR "Shimovolos v. Russia", Application no. 30194/09, 21 June 2011, <http://hudoc.echr.coe.int/eng?i=001-105217>, concerning the registration of a human rights activist in a "surveillance database", which collected information about his movements by domestic train or air travel.

141 See, ECtHR "Catt v The United Kingdom" Application no. 43514/15, 24 January 2019, <http://hudoc.echr.coe.int/eng?i=001-189424>, which concerned the collection and retention of data about a lifelong activist in a police database for "domestic extremists".

142 See e.g., ECtHR "Brunet v. France" Application no. 21010/10, 18 September 2014, <http://hudoc.echr.coe.int/eng?i=001-146389>.

143 See e.g., ECtHR "Khelili v. Switzerland" Application no. 16188/07, 18 October 2011, <http://hudoc.echr.coe.int/eng?i=001-107032>.

144 See, Human Rights in Counter-Terrorism Investigations – A Practical Manual for Law Enforcement Officers, (Warsaw/Vienna: OSCE/ODIHR, 2013) p. 30, <https://www.osce.org/files/f/documents/5/f/108930.pdf>.

145 Just as sharing API, PNR or biometric data across borders can create new or exacerbate existing threats to human rights.

146 UN Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, UN Doc. A/HRC/25/60, 10 April 2014, para 76, <https://undocs.org/A/HRC/25/60>.

to a state where there is a real risk that this information is used in violation of international human rights law, can make the sending state complicit in those violations. Therefore, states should verify the existence and observance of effective human rights safeguards in the co-operating state before sharing data with or receiving data from authorities in another country.[147]

UNSC Resolution 2396 calls on states to make regular use of Interpol databases for screening travellers at air, land and sea ports of entry.[148] Many have sounded the alarm about the potential for abuse of Interpol red notices and so-called "diffusions" (i.e., other law enforcement co-operation requests) about wanted persons as a tool to "export oppression" or their "weaponization" against government critics.[149] The impact this can have on people, including migrants, refugees and asylum seekers, is evident and has been well-documented.[150] Efforts by Interpol to address the problem and protect itself from misuse of its mechanisms have been broadly acknowledged.[151] But the potential for abuse remains high and challenges persist. In this context, the need for Interpol to further strengthen scrutiny of notices and diffusions, and accountability for states that abuse the system has been highlighted by international bodies and civil society.[152]

As the Parliamentary Assembly of the Council of Europe (PACE) highlighted, "[i]nternational co-operation in the field of criminal law requires a high degree of mutual trust, based on common standards and practices."[153] A lack of respect for human rights undermines trust, co-operation between states (both bilateral and multilateral) and, as a result, also joint efforts to counter-terrorism and other transnational threats.

147 UN Special Rapporteur on counter-terrorism, "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight", UN Doc. A/HRC/14/46, 17 May 2010, Practice 33, <https://undocs.org/A/HRC/14/46>. See, Guidelines for Addressing the Threats and Challenges of 'Foreign Terrorist Fighters' within a Human Rights Framework, *op. cit.*, note 5, pp. 34, 42 and 43.

148 UNSC Resolution 2396 (2017), para 16.

149 See e.g., PACE Resolution 2315, *op. cit.*, note 136; PACE Resolution 2161 "Abusive use of the Interpol system: the need for more stringent legal safeguards", 26 April 2017, <https://pace.coe.int/en/files/23714/html>; Fair Trials "Dismantling the Tools of Oppression: Ending the Misuse of INTERPOL", 4 October 2018, <https://www.fairtrials.org/sites/default/files/publication_pdf/Dismantling%20the%20tools%20of%20oppression.pdf> and Fair Trials "Strengthening respect for human rights, strengthening INTERPOL" 26 November 2013, <https://www.fairtrials.org/publication/strengthening-respect-human-rights-strengthening-interpol>, Nate Schenkkan and Isabel Linzer, "Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression", Freedom House, February 2021, with case studies on Russia, Turkey and other countries, as well as regional snapshots from across the world, <https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf>.

150 For specific case examples see, Fair Trials "Dismantling the Tools of Oppression", *ibid.* In this context it is also worth noting that other Interpol mechanisms, such as the database for lost and stolen travel documents, have reportedly been used for similar purposes (see Freedom House, February 2021, *ibid.*). Furthermore, as pointed out by PACE, other interstate mutual legal co-operation mechanisms, such as the Schengen Information System, can be subject to misuse and may result in violations of privacy, property, professional rights and deprivation of liberty, see PACE Resolution 2315, *op. cit.*, note 136, para 5.

151 For example, the strengthening of the Commission for the Control of Interpol's Files (CCF), to which people targeted by notices and diffusions may appeal. See PACE Resolution 2315, *op. cit.*, note 136, para 7, and Fair Trials "Dismantling the Tools of Oppression", *op. cit.*, note 149.

152 See PACE Resolution 2315, *op. cit.*, note 136, paras 8 and 10.1. As measures to prevent abuse of Interpol instruments are strengthened, states should also be alert to the use of alternative mechanisms, which do not provide similar protections and states may use instead to target government critics abroad. See, Fair Trials "Dismantling the Tools of Oppression", *op. cit.*, note 149, pp. 67-68.

153 PACE Resolution 2315, *op. cit.*, note 136, para 4.

- Before entering into **information sharing agreements** with other countries, or sharing information on an ad hoc basis, an assessment should be made of the **counterpart's record on human rights and data protection**.[154]
- In multilateral information sharing, states need to remain vigilant to co-operation requests from states with poor human rights and rule of law records, including a lack of independent prosecution and courts, and take effective steps against the abuse of such co-operation requests.[155]

154 This recommendation has been made by the UN Special Rapporteur on counter-terrorism, Martin Scheinin, in relation to exchange of information between intelligence agencies, but it should apply to all information sharing between states, including API/PNR, biometric or other data for law enforcement purposes. See UN Special Rapporteur on counter-terrorism, "Compilation of good practices", *op. cit.*, note 147, Practice 33.

155 See PACE Resolution 2315, *op. cit.*, note 136, paras 9.6, 10.1. and 10.2.

Conclusion

While states have the right to control who enters their territory and an obligation to counter terrorism and other crime, this must be done in full compliance with international human rights standards. The emergence and growing use of new border management technologies that gather and process large amounts of personal data to track, identify and control those crossing borders[156] poses new challenges for the protection of human rights. Technology is far from neutral.[157] Placing people under suspicion based on assumptions generated by algorithms, discriminatory profiling, surveillance, and privacy and other human rights infringements resulting from the collection, processing and sharing of biometrics, API/PNR and other travel-related data are just some of the human rights risks such technologies entail.

These risks are amplified by a lack of transparency and oversight of systems developed for border management; and they put people in particular situations of vulnerability, such as migrants, asylum seekers and refugees, especially at risk. Over-securitized border management, which denies people their rights and targets those who are in most acute need of protection, will lose the trust of the communities it should serve. Consequently,it will not create more security but less. Human rights protections are a vital tool to ensure effective cross-border security.

Therefore states are urged to:

- Put in place a robust **legislative framework** that regulates the use of new technologies at borders and provides strong **human rights safeguards;** and ensure that these safeguards are integrated into all related international and transnational co-operation agreements, including in relation to data sharing;
- Be transparent and accountable about the development and use of technological tools and systems for the collection, processing and sharing of personal data in border management and security;
- Establish effective and **independent external oversight** mechanisms, regular monitoring and review, as well as effective remedies for those whose rights are affected;
- Make **human rights due diligence mandatory** and ensure that thorough **human rights impact assessments** are conducted in the development of and prior to deployment of any such technology, and at regular intervals in its operation by those developing, procuring and operating the systems, to assess, and where necessary, mitigate human rights risks;
- Ensure that such **assessments are participatory**, involving non-governmental organizations reflecting the diversity of society, as well as groups and communities whose rights are most affected; and
- Ensure that border guards and others using new technology systems receive adequate **human rights training** and are sensitized to potential bias and human rights implications of the systems.

156 "Technological Testing Grounds" *op. cit.*, note 19, p. 2.
157 *Ibid.*, p. 37.

Furthermore, states should **refrain from global proliferation** of technology that has detrimental human rights impact, through export and official development assistance.

While states have the primary obligation to respect and protect human rights, **private business enterprises** also have human rights responsibilities to which they need to be held accountable – especially when they develop or apply such technology or are otherwise involved in or directly perform border management-related functions.

Follow OSCE and ODIHR

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10
00-251 Warsaw
Poland

Office: +48 22 520 06 00
Fax: +48 22 520 06 05
office@odihr.pl