.

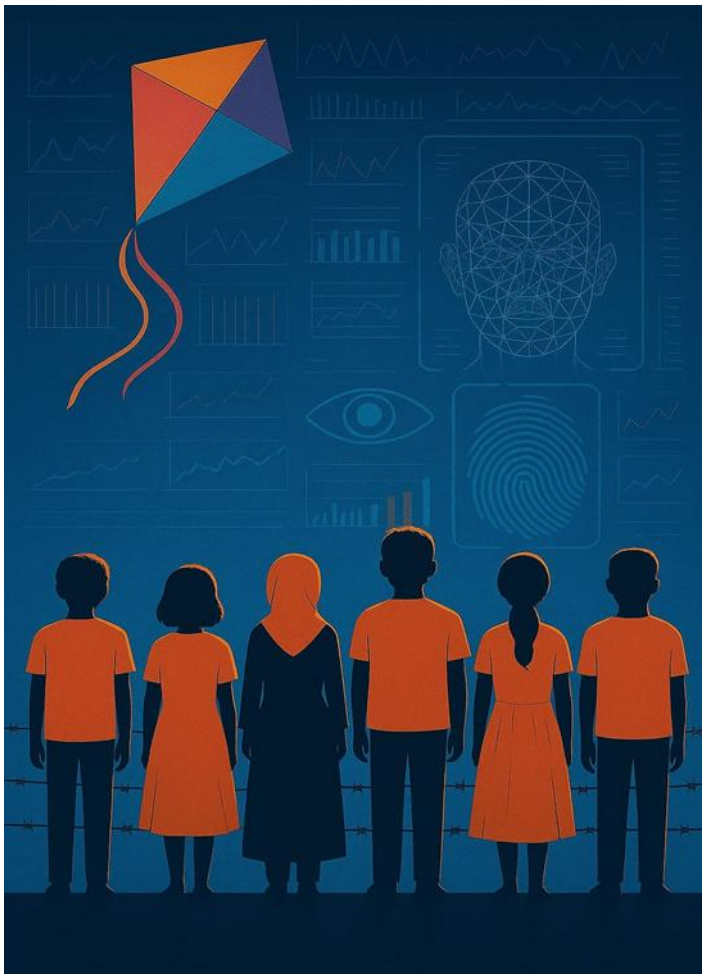
Collecting Children's Personal Data for Counterterrorism Purposes: In Children's Best Interests?

Children with Alleged, Past, or Family Links to Armed Groups

Discussion Paper

Daniela Baro*

May 2025



* This Discussion Paper was written while the author was a fellow at the University of Essex Human Rights Centre. The author is grateful for the support of the Human Rights Centre with this research. The Discussion Paper is written in a personal capacity, and any errors and omissions remain those of the author.

.

Table of Contents

.

Introduction

Over the past two decades, counter-terrorism measures and agencies have dramatically expanded,[1] particularly with the sweeping collection of personal data for counterterrorism purposes. Children have not been exempted from these measures. Human rights experts have pointed out a troubling oversight in how these policies are implemented: there is a consistent "lack of attention to the necessary protections due to the child" in counter-terrorism efforts, including in both bilateral and multilateral counter-terrorism technical assistance.[2]

Counter-terrorism policies have included measures like lowering the minimum age of criminal responsibility for certain terrorism-related offenses, trying children in military or specialized counter-terrorism courts, and even applying the death penalty for terrorist acts committed by children.[3] Thousands of children have been deprived of liberty on national security grounds in military, administrative or pre-trial detention, often for long periods. Children are detained not only for being allegedly associated to armed groups designated as terrorist groups but also based on the suspicion that they might be sympathetic to such groups or have family members involved.[4]

In 2023, over 3,000 children in 11 countries were detained for suspected ties to armed groups,[5] and in 2024, approximately 29,000 remained interned without any charges or individual review in the Al-Rawj and Al-Hawl camps in north-eastern Syrian Arab Republic[6], due to alleged family connections to the armed group Islamic State in Iraq and the Levant (ISIL, also known as Da'esh).[7] The consequences for these children can be devastating. Many face ill-treatment, appalling detention conditions, and violations of their due process rights.[8]

UN Security Council resolutions have mandated the collection of personal data, including biometric data, and the exchange of information related to watchlists or databases of known and suspected terrorists, including Foreign Terrorist Fighters and their families, with no exception for spouses or children under 18 years.[9]

This raises critical questions: to what extent is children's personal data being gathered and used for counterterrorism purposes? What impact does this have on children´s lives and human rights? Is their personal data adequately protected within counterterrorism regulatory frameworks? This paper dives deep into these issues.

The topic of security-related personal data collection is large and given the sensitivity and opacity of the issue, access to information is limited. Therefore, I narrowed the research scope to two often-overlooked groups in this

---

[1] "The Datification of Counterterrorism" by Fionnuala Ní Aoláin in *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold,* 2022.

[2] *Position Paper of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism on the Rights of Children in Contexts affected by Counter-Terrorism*, Professor Fionnuala Ní Aoláin, October 2023.

[3] https://childrenandarmedconflict.un.org/2024/09/somalia-un-officials-alarmed-at-execution-of-four-young-people-for-crimes-committed-as-minor-call-for-release-reintegration-of-children-in-detention/; *Position Paper of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism on the Rights of Children in Contexts affected by Counter-Terrorism* by Professor Fionnuala Ní Aoláin, October 2023.

[4] *Global study on children deprived of liberty,* 11 July 2019, A/74/136, para. 93.

[5] *Children and armed conflict, Report of the Secretary-General*, 3 June 2024.

[6] The Al-Hawl camp (also Al-Hol) is a camp in north-east Syria close to the Syria-Iraq border, which holds primarily the wives, adult females and children of male ISIL suspects. As of September 2022, of the 56,000 persons held in the camp 28.000 were from Iraq and over 10,000 from 60 other nations; over 60 % were children. See "*My son is just another kid",* Human Rights Watch, 2022.

[7] *Punishing the innocent: ending violations against children in the north-east of the Syrian Arab Republic* by the Independent International Commission of Inquiry on the Syrian Arab Republic, March 2024; *Children and armed conflict, Report of the Secretary-General*, 3 June 2024; interview with UN worker in MENA region.

[8] *Global study on children deprived of liberty*, 11 July 2019, A/74/136, paras. 74-78. See also "*We dried our tears". Addressing the toll on children of northeast Nigeria's conflict*, Amnesty International, 2020; *They Didn't Know if I was Alive of Dead,* Human Rights Watch, 2019.

[9] S/RES/2178 (2014); S/RES/2396(2017) paras. 5, 16, 22 and 29.

.

context: children formerly or allegedly associated with armed groups designated as terrorist in (post-) conflict settings, and children whose family members are suspected of such affiliations, such as children of "foreign terrorist fighters".

Regarding children associated with armed groups, policy, research and practice largely focus on pressing prevention and reintegration needs—addressing why they join and leave armed groups, and how they are reintegrated. Security-led data collection on these children receives little attention. In the case of children with family ties to terrorist-designated armed groups, the emphasis of research and advocacy has understandably been on their detention, dire conditions, and on their repatriation and reintegration, rather than on issues related to their personal data.

This research does not cover other groups of children also subject to counterterrorism measures including personal data collection or surveillance, such as children considered at risk of "radicalization"[10] due to their perceived beliefs, often targeted by preventing or countering violent extremism (PVE/CVE) programs.[11]

The paper provides examples of children´s data collection practices in several countries from Africa and Middle East regions (Lake Chad Basin, Somalia, Iraq and Syria), the U.S. and Europe, drawing from (online) interviews with (80) experts in counterterrorism, data protection, and child protection, as well as from a desk review and analysis of relevant standards, research, and policy documents.

The goal is to prompt counterterrorism policymakers to consider the broader implications of their actions on children's rights, particularly when it comes to the collection and use of children´s personal data. Ultimately, it is aimed at putting the best interests of children at the front and center in policies concerning personal data related to counterterrorism. To that end, this discussion paper raises some concrete options as possible way forward.

The paper begins by explaining why the collection of children's personal data for counterterrorism purposes warrants special attention (I). It then outlines key challenges that hinder the protection of children's rights in this context (II). Next, it provides examples of children's data collected in counterterrorism settings, from those formerly or allegedly associated with armed groups designated as terrorist, as well as children with family ties to such groups (III). The paper then examines data sharing and watch listing practices (IV), followed by examples of the potential harm these practices may cause to children (V). It goes on to analyze how relevant regulatory frameworks address children's data, with a focus on child rights protections under international human rights law (VI). Finally, it discusses possible options for concrete, rights-based safeguards to strengthen the protection of children's personal data in counterterrorism contexts (VII). Annex I provides some country-specific examples of security-led personal data collection involving children. Annex II outlines child-related provisions in key regulatory frameworks dealing with data protection and counterterrorism.

Definitions

Children

In line with the United Nations Convention on the Rights of the Child, a child is any human being below the age of 18 years.[12]

[10] As with the concept of 'terrorism,' there is little consensus among scholars and policymakers on the precise meaning of the term 'radicalization' (UNICRI). The interpretation of the term "radicalization" can be quite broad by lack of a clear definition, this leading to ambiguity in policy and interventions (UNODC). https://www.unodc.org/e4j/en/terrorism/module-2/key-issues/radicalization-violent-extremism.html

[11] See, for example, Prevent programme in the UK. *The People's Review of Prevent*, February 2022; "Family wins fight to delete child from Met's anti-radicalization records" at https://www.theguardian.com/uk-news/2019/dec/19/family-wins-fight-to-delete-child-from-met-prevent-anti-radicalisation-records?awc=5795_1579116458_8d743013b3221b8e2da471942473ddf8

[12] Article 1 of the UN Convention on the Rights of the Child (CRC).

.

Adolescents
For the purpose of this study, adolescents are children between the age of 10 and 18.[13]

Armed groups
Armed groups that are distinct from the armed forces of a State in armed conflict situations.[14]

Terrorist groups
There is currently no universally agreed definition of "terrorism" or "terrorist group".[15] For the purpose of this study, the term "terrorist group" encompasses at least the armed groups designated and listed as terrorist groups by the UN Security Council, including ISIL (Da´esh), Boko Haram, and Al-Shabaab.

Children associated with armed groups
All children who have been recruited and exploited by armed groups, including by armed groups designated as terrorist groups.[16]

Foreign Terrorist Fighters
Individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict.[17]

Personal data
Personal data is herein understood as any information relating to a natural person ('data subject'), who can be identified, directly or indirectly, particularly through an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[18]

Biometric data
Biometric data consists of data uniquely identifying biological characteristics of a person like digital images, a person's gait, voice recognition, iris patterns, DNA, or fingerprints.[19] Biometric data enables a more accurate identification of individuals, as it prevents concealment using false identities like fake documents or name changes.[20]

---

[13] According to the World Health Organization, adolescence is the phase of life between childhood and adulthood, from ages 10 to 19. https://www.who.int/health-topics/adolescent-health/#tab=tab_1
[14] Definition in A/RES/54/263 (2001). Article 1(1) of the 1977 Additional Protocol II to the Geneva Conventions, applicable in internal armed conflicts, refers to "organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations".
[15] Each UN Member State has the prerogative to define terrorism, in a way "that must be consistent with their obligations under international law and in particular international human rights law." *Report of the United Nations Secretary-General, Plan of Action to Prevent Violent Extremism*, A/70/674, para.5.
[16] The United Nations Global Counter-Terrorism Strategy: Seventh Review resolution A/75/291 mentions "children formerly associated with armed groups, including terrorist groups, as guided by the Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (the Paris Principles)", para. 117.
[17] UN Security Council resolutions 2178 (2014), 2253 (2015), 2396 (2017).
[18] Article 3.1 of the EU Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001.
[19] EU General Data Protection Regulation (GDPR), Article 14.
[20] https://www.interpol.int/Crimes/Terrorism/Identifying-terrorist-suspects

.

Summary of key findings

This research delves into a highly pressing issue: the collection and use of children's personal data for counterterrorism purposes, and the resulting impact on their human rights. Given the sensitive nature of the topic, a main challenge has been the lack of tangible evidence on the extent of this data collection, its usage, and its transfer—particularly when it comes to children formerly recruited by or allegedly associated with armed groups, or those with family links to armed groups labeled as terrorist groups. This opacity itself is a significant finding, highlighting a gap in our understanding of how children's personal data is handled in counterterrorism efforts within (post) conflict settings. Other key findings are outlined below.

- The recruitment and use of children by non-state armed groups continues to be a prevalent feature of armed conflicts. Some of these armed groups are labelled as terrorist groups.[21] This labelling is often driven by political considerations rather than a universally agreed legal framework defining terrorism. States frequently view children recruited by armed groups, particularly those designated as terrorist groups, as security threats, and largely fail to consider the circumstances of extreme duress and coercion that lead many children to become associated with these groups.[22] As a result, thousands of children who have been unlawfully recruited or exploited by these groups are detained on national security grounds—often solely due to their actual or perceived membership in such groups. Even children with family ties to terrorist-designated armed group members can find themselves imprisoned simply because of their family connections.
- Both children exiting armed groups labeled as terrorist and those detained due to national security concerns have been subject to data collection by security forces or agencies in various (post) conflict contexts, such as Syria, Iraq, Somalia, and Lake Chad Basin countries.
- But what happens to this data? Once it is collected, it is often stored and potentially shared across watch lists and surveillance systems.[23] The creation of these watch lists typically occurs without judicial oversight, leaving security bodies with immense, unchecked power. Children—due to their perceived vulnerability to recruitment—may be included in these lists, yet the secrecy surrounding the process makes it hard to gauge how widespread or accurate the listing is.
- What is certain, however, is the vast and growing flow of information between national, regional, and international databases. Security agencies now cross-check biographic and biometric data with information systems containing records of flight passengers, migrants, and asylum seekers. The UN Security Council Executive Directorate (CTED) has highlighted that "States have increasingly developed terrorist watch lists and databases that link or crosscheck with biometric databases,"[24] suggesting a web of interconnected data that can potentially put children at risk without their knowledge.
- What does this practically mean for children? Once their data is shared with various agencies—immigration authorities, police, or even international agencies, each with its own data retention, sharing and erasure policies —the implications can be far-reaching. Children may be unaware that their personal data is stored or shared, potentially encountering barriers in their future lives, such as at airports, schools, or workplaces. Worse still,

[21] The UN Security Council ISIL (Da'esh) and Al-Qaida Sanctions Committee has listed over 50 armed groups and organizations as terrorist organizations in accordance with paragraph 13 of Security Council resolution 1822 (2008) and subsequent related resolutions. Some UN Member States publish a list of armed groups and organizations they have designated as terrorist organizations. The EU has also listed armed groups designated as terrorist groups. See examples at https://en.wikipedia.org/wiki/List_of_designated_terrorist_groups

[22] "'I Am Nothing Without a Weapon', Understanding Child Recruitment and Use by Armed Groups in Syria and Iraq" by Mara Revkin in *Cradled by Conflict*, United Nations University, 2018.

[23] Surveillance can encompass bulk collection of metadata and biometric data; electronic surveillance may consist of wiretapping, monitoring of emails, social media profiles, digital cloud storage, drones or unmanned aerial systems, and the use of physical electronic trackers. See *Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space* by Annabelle Bonnefont, Global Center on Cooperative Security, March 2024.

[24] *Analytical Brief: Biometrics and Counter-Terrorism*, Security Council Counter-Terrorism Committee Executive Directorate (CTED). https://www.un.org/securitycouncil/ctc/content/cted-analytical-brief-biometrics-and-counter-terrorism

.

the process of removing or correcting this data is complex, too often onerous and inaccessible to those affected, especially if too much onward sharing has taken place.[25]

- This data collection can cause disproportionate and life-long harm to children. They could face interrogation, detention, family separation, denial of education, travel bans, refusal of asylum or exclusion from jobs or social benefits, in addition to stigmatization. The repercussions for young children of "foreign terrorist fighters" repatriated to their home countries from Syria and Iraq are still unfolding, with potential, in some cases, for long-term surveillance, rights restrictions and/or stigma.
- At the same time, current counterterrorism regulations often fail to address the unique vulnerabilities of children. Counter-terrorism laws are often "age-blind," without a distinction between children and adults when dealing with individuals recruited by terrorist organizations.[26] Many of these frameworks are either silent or too vague about the protection of children's personal data. Key challenges are also the lack of a universally agreed definition of "terrorism" (and of "violent extremism"), and broad interpretations of the concept of "association" with an armed group.
- In sum, against today´s global trend of widespread collection of personal (and biometric) data and of pervasive counterterrorism measures, the vulnerability of children is ever growing. This underlines a pressing need for stronger protections for children's rights when it comes to the collection and sharing of children´s personal data in the context of counterterrorism. It is crucial for professionals in both data protection and child protection fields to recognize the intersections of these areas and work together to safeguard children's rights in counterterrorism environments. Particularly those working on child protection in conflict situations, need to pay closer attention at the collection and use of children's personal data for counterterrorism purposes, and to further search and document the impact of such practices on children's lives.
- More broadly, it seems imperative to find ways to bridge the gap between enhancing security and child rights´ protection.[27]

I. Why focus on children´s personal data linked to counterterrorism ?

Two key reasons for focusing on children´s personal data in counterterrorism settings lie on children´s vulnerability and poor visibility in these contexts. Children are not only particularly vulnerable to having their personal data collected on national security grounds without their knowledge, but also the consequences of their inclusion in security databases can increase their vulnerability. Also, children's rights appear to be rare in research and policy debates about personal data in counterterrorism (post) conflict scenarios.

Vulnerability of children

The right to privacy is not absolute. States may lawfully restrict it for legitimate security or defense interests, provided such measures are necessary and proportionate. So, members of armed groups—especially those designated as terrorist—may have their personal data lawfully collected for national security purposes. However, the case of children associated with armed groups requires distinct treatment: they are first and foremost victims of unlawful recruitment and exploitation.

Child psychology suggests that children are more susceptible to manipulation than adults due to a combination of factors linked to their cognitive and emotional development.[28] Neuroscience research even confirms that brain

[25] *Prevent and the Pre-crime State: How unaccountable data sharing is harming a generation,* Open Rights Group, February 2024.
[26] *Strengthening Human Rights in Counter-Terrorism Strategy and Policy: A Toolkit*, UN Office of the High Commissioner for Human Rights.
[27] There is a perceived dichotomy between security and children's rights, and a need to breach this gap at capacity building, policy, and institutional levels. Discussion with UNODC.
[28] https://psychcentral.com/news/2018/05/27/modeling-behavior-for-children-has-long-lasting-effects#1. The Preamble of the UN Convention on the Rights of the Child acknowledges that "the child, by reason of his physical and mental immaturity, needs special safeguards and care, including appropriate legal protection…".

.

development continues into the person´s twenties.[29] Because of their immaturity and easier manipulation children are targeted for recruitment by armed groups, including those designated as terrorist groups. Commanders reportedly often see children as "very good soldiers …[because] they obey orders; they are not concerned about getting back to their wife or family; and they don't know fear"…Others argue that it is not that children are fearless, but rather that they cannot fully grasp the inherent danger of combat".[30] For instance, the Lord Resistance Army´s preference for younger recruits is chillingly clear in the testimony of a local priest: "They now want younger children, those whose minds can be transformed in a matter of weeks."[31] Poor socio-economic conditions in conflict situations, and new means of warfare, can all facilitate this targeting of children.[32]

Beyond being recruited, children associated with armed groups frequently suffer from further human rights violations in the hands of armed groups. These include exploitative labor, inhumane treatment, forced marriage, sexual slavery, abduction and trafficking.[33] Yet, the law may criminalize these children who were in the first place unlawfully recruited and exploited. Some countries criminalize the sole membership in a terrorist organization or interpret the law broadly to include not only direct participation in terrorist acts, but also mere association.[34] As a result, these children risk being victimized twice: first by armed groups, and again by being labeled security threats and having their data treated accordingly.

Further, children in counterterrorism contexts often lack official identity documents due to forced displacement or lack of birth registration.[35] Without proof of age, adolescents, especially boys considered to be "military-age males", may be treated as adult fighters and thus exposed to risks of being targeted, or caught in security oriented

---

[29] "Development of the adolescent brain: implications for executive function and social cognition" by Sarah J. Blakemore and Suparna Choudhury, *Journal of Child Psychology and Psychiatry*, vol. 47, Nos. 3–4 (March/April 2006), pp. 296–312; "Structural and functional brain development and its relation to cognitive development" by B.J. Casey, J.N. Giedd and K.M. Thomas, *Biological Psychology*, vol. 54, Nos. 1–3, (October 2000), pp. 241–257, cited in *UNODC Manual on An Ecological Framework for Psychosocial Child Assessment*, 2023.

[30] For instance, an 18-year-old Iraqi boy who joined ISIL indicated that trainers seemed to view children as ideal candidates for suicide missions because of their enthusiasm. In ""I Am Nothing Without a Weapon", Understanding Child Recruitment and Use by Armed Groups in Syria and Iraq" by Mara Revkin in *Children and Extreme Violence: Cradled by Conflict,* United Nations University, 2018, p. 130.

[31] *Indoctrinate the Heart to Impunity: Rituals, Culture and Control within the Lord's Resistance Army,* Harvard Humanitarian Initiative, Nov. 2015. The Lord Resistance Army (LRA) abducted thousands of children into its ranks "in large part because they are easier to manipulate than adults. Through fear, mind-control methods and sheer brutality, the LRA has initiated children into its ranks and forced them to undergo what it refers to as 'military training.'" See https://www.hrw.org/news/2015/01/09/questions-and-answers-lra-commander-dominic-ongwen-and-icc

[32] https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0824.pdf; *Cradled by Conflict, Understanding child recruitment by armed groups, including terrorist organizations, and identifying obstacles to releasing children from such groups,* United Nations University, February 2018; https://childrenandarmedconflict.un.org/2023/02/questions-and-answers-on-the-recruitment-and-use-of-child-soldiers2/

[33] The *U.S. Department of State Country Reports on Terrorism* (2023) reports that "since at least 2015, the group (ISIS) has integrated local children and children of FTFs into its forces and used them as executioners and suicide attackers. ISIS has systematically prepared child soldiers in Iraq and Syria using its education and religious infrastructure as part of its training and recruitment of members. ISIS also has abducted, raped, and abused thousands of women and children, some as young as 8 years old. Women and children were sold and enslaved, distributed to ISIS fighters as spoils of war, forced into marriage and domestic servitude, or otherwise subjected to physical and sexual abuse".

[34] Examples of legal systems criminalizing or broadly interpreting membership include Iraq, Article 4(1) of the Anti-Terrorism Law No. 13 (2005); France, Article 421-2-1 of the French Penal Code (Code pénal); Nigeria, Terrorism Prevention Act (TPA) (2011), Section 5(1); Afghanistan, Law on Combat against Terrorist Offences, Sections 91(1) and 3(2); Egypt, Art. 12 of Law No. 94 of 2015 on Combating Terrorism; United Kingdom Terrorism Act 2000, Section 11; Australia, Criminal Code Act 1995, Division 102; Germany, Section 129a of the German Criminal Code (Strafgesetzbuch); Turkey, Art. 314 (2) of the Turkish Penal Code (Türk Ceza Kanunu – TCK). See *An international survey of anti-terrorism legislation and its impact on children*, Child Rights International Network (CRIN), 2018*; Report on visit to France by former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Fionnuala Ní Aoláin*, 2019, para. 30.

[35] This is the case, for instance, in the Democratic Republic of Congo, Nigeria, Somalia and South Sudan. See *The State of the World's Children* annual report, UNICEF 2023; https://www.unicef.org/protection/birth-registration; *Civil Registration in Humanitarian Contexts, Recommendations and Operational Guidelines for African Union Member States*, UNICEF 2023.

.

data collection. The category of "military age males" is a way of conflating children with adults in a way that excludes them from protection. (See personal data collection by the U.S. army in Iraq and Afghanistan in Annex I).

This issue of age is further complicated by the discrepancy between legal definitions and societal perceptions of childhood. In countries like Iraq, where the legal age of majority is 18,[36] societal norms often regard boys and girls as adults much earlier, engaging in early marriages or being recruited by armed groups. The recruitment and use of children under 18 by different armed groups and militias has been a common feature of conflict in Iraq,[37] and authorities allegedly consider fighting age at 14.[38] The armed group ISIL exacerbated this treatment of children as adults. For example, adolescent boys recruited into the group were allegedly offered rewards as other adult fighters, such as administrative positions, even houses and brides.[39]

Yet the vulnerability of children extends beyond recruitment. Adolescents tend to be less guarded when expressing their views and may unknowingly fall victim to broad, vague domestic legal definitions of terrorist acts, such as ´apology for terrorism´ or contribution (even if relatively remote) to supporting a terrorist group. In France, for instance, the law criminalizing the apology for terrorism has been widely criticized for its vagueness and its wide use against children.[40] As noted by the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Professor Fionnuala Ní Aoláin, 85 per cent of criminal cases related to terrorism in France were based on this charge, and she was particularly concerned that it had been used extensively against children.[41]

Finally, children are vulnerable to being drawn into the sphere of terrorist groups through their parents and thus unintentionally suffer the consequences of their parents´ choices. Thousands of children remain deprived of their liberty in Syria and in Iraq due to their parents´ real or presumed association with armed groups designated as terrorist. While these children are largely recognized as innocent, they are also often treated by States and communities as security threats, leading to their further marginalization.[42] These children face or risk double victimization: first by their parents' choices, including by being taken to dangerous conflict zones, and again by being treated as threats due to their family ties.

The above vulnerabilities heighten the risk of children's personal data being collected and used for counterterrorism purposes. Also because of these vulnerabilities, children´s data require greater protection.

Poor visibility of children´s data protection in counterterrorism contexts

The collection and use of children's personal data for counterterrorism purposes in conflict zones, is an area that has received surprisingly little attention. Advocates and researchers consulted for this study, and child protection actors who have directly engaged with children formerly associated with armed groups, including those designated as terrorist groups such as Boko Haram and Al-Shabaab, report a critical gap in this field.

Research on biometric data collection and data flows in counterterrorism contexts rarely specifically addresses whether children's data is included. This may be due to, at least, two main factors: in many conflict settings,

---

[36] Iraq Civil Code No. 40 (1951), Arts. 106 and 97 para. 2.

[37] Secretary General reports on children affected by armed conflict, Iraq section, Library – Office of the Special Representative of the Secretary-General for Children and Armed Conflict (un.org)

[38] *The Limits of Punishment, Transitional Justice and Violent Extremism*, United Nations University, May 2018, p. 65.

[39] Interviews conducted by the author in 2022 with personnel from organizations assisting children in Iraq. An interviewee reported the case of a 13-year-old boy to whom ISIL allegedly offered to choose a girl as bride and took him to a court to get married.

[40] *Children, the justice system, violent extremism and terrorism: An overview of law, policy and practice in six European countries*, International Juvenile Justice Observatory (IJJO), October 2018, p. 11.

[41] *Report on visit to France by former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Fionnuala Ní Aoláin* (A/70/371, 2019), paras. 29, 31-44.

[42] Interview with former UN worker in Syria.

.

security actors often view adolescents in armed groups as any other (adult) fighters - not as children - and therefore may not highlight their distinct situation. At the same time, there is also a frequent tendency to think of children primarily as young dependents—often with mothers or carers—rather than as adolescents with agency. As a result, researchers may have neither received nor actively sought information about children, likely perceived as marginal to security-focused research.

Actors who do focus specifically on children, such as child protection humanitarian workers, often have little or no detailed information about the collection of children's data for security purposes, due to the sensitivity and opacity of the issue. Child protection actors consulted said that, when interacting with children disengaging from armed groups, they did not systematically ask about the collection of personal data upon their capture or reception by security forces. Did these children have their photos taken? Were their fingerprints recorded? Were they informed about the purpose of such data collection? These questions seem rarely to be raised.[43] In a survey conducted among child protection practitioners on issues concerning children associated with armed forces and armed groups, data protection and the actual or potential collection of children´s personal data on security grounds were reportedly not raised at all.[44]

Understandably, child protection efforts have prioritized the most visible serious child rights concerns, along with the most pressing reintegration needs. In contrast, security-led data collection on children is less visible (or often hidden), as are its consequences. Yet it may equally have a long-term impact on children. Additionally, a forward-looking focus on data collection and privacy could be an entry point to address other pervasive issues like discrimination or surveillance targeting certain groups of children because of their race, nationality, religion, family or community links, or help prevent further abuses like arbitrary detentions of those children.

At the same time, national and regional counterterrorism laws and regulatory frameworks often leave the collection and use of children's personal data in a state of ambiguity. For example, the EU's Regulation on the Schengen Information System, offers no specific protections for children when it comes to alerts related to suspected terrorists.[45] Or consider NATO's Policy on Children and Armed Conflict,[46] which remains silent on the issue of biometric data collection or the protection of children´s personal data in conflict zones – despite NATO's policy development on biometric data and guidance on the collection of battlefield evidence.[47]

Similarly, counterterrorism bodies that assist States with training and in developing counterterrorism policies are not necessarily addressing how data collection measures affect children. For example, while the renewed mandate of the UN Security Council's Counterterrorism Executive Directorate, as a welcome positive development, now includes assessing the impact of terrorism on children,[48] it does not include assessing the impact of counterterrorism measures on children—even though such measures have led to serious violations of children's rights, including arbitrary detentions and denial of due process.

In addition to the above poor visibility, there are also key challenges in protecting children´s rights and data, which include the vague and inconsistent definitions of "terrorism" and of "association" with armed groups, as well as the exemptions from most data protection obligations and rights when data is collected for national security or defense purposes, as discussed below.

---

[43] Interviews with researchers on children and armed conflict in Somalia and the Lake Chad Basin.
[44] Interview with child protection INGO.
[45] Schengen Information System (SIS) Regulation; interview with Niovi Vavoula.
[46] *NATO Policy on Children and Armed Conflict* (last updated: 14 Jul. 2023) https://www.nato.int/cps/en/natohq/official_texts_217691.htm
[47] https://www.nato.int/cps/en/natohq/topics_77646.htm?selectedLocale=en; https://www.ncia.nato.int/videos/nato-automated-biometric-identification-system-nabis.html.
[48] S/RES/2617 (2021), para. 37.

.

II. Key challenges

Conceptual vagueness

The elusive definition of terrorism

Despite decades of international debate, no universally accepted definition of terrorism exists.[49] States often apply the term largely based on their national and foreign policy priorities. In fact, the listing or de-listing of an armed group as "terrorist" can occur with little change in the group's *modus operandi*, driven more by political considerations than by objective criteria.[50] This labelling, hence, tends to shift depending on national or regional political shifts. Even opposition groups or political adversaries may be branded and treated as terrorists,[51] and acts of dissent or legitimate protest be considered as terrorist acts.[52]

But, most importantly, regardless of how an armed group is labeled or designated, the psychological and social impact on children of being recruited and used by the armed group—and the children´s rehabilitation and reintegration needs—remain the same.[53]

Expanded meaning of association

What seems pressing on data collection though is the association with an armed group, even if the armed group is not designated as terrorist. Association appears to be the entry point.[54]

Yet not only is the notion of terrorism broadly and inconsistently understood, there is also increasingly in counterterrorism contexts a broad interpretation and misuse of the concept of "association" to an armed group. For instance, a narrative that is getting traction especially among State officials in the Lake Chad Basin, the Sahel and Horn of Africa regions, is to include as "association" the fact of living in the territory controlled by armed groups.[55] So, if people have been held in areas under the territorial control of an armed group, they may be automatically deemed associated to the armed group.[56] But when entire communities, including children, are labeled as suspects due to their geographical location, are we not undermining the principles of individual criminal responsibility and the presumption of innocence? These blanket assumptions may also contribute to cycles of stigma and revictimization.[57]

The gendered dimensions of such broad interpretations of association are equally troubling. As noted by former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ms. Fionnuala D. Ní Aoláin, "women and girls kidnapped, coerced or groomed into terrorist organizations, are often viewed as supporters or enablers of terrorism rather than *prima facie* victims of terrorism".[58]

---

[49] *United Nations Integrated DDR Standards* (IDDRS 2.10 The UN Approach to DDR).
[50] *Disarmament, Demobilization and Reintegration (DDR) & Armed Groups Designated as Terrorist Organizations (AGDTO)*, Whitepaper, United Nations, DRAFT updated 27 June 2024.
[51] Interview with Yasha Maccanico from Statewatch.
[52] See examples of terrorism listing of human rights defenders and activists in Israel and Egypt in *Terrorism and human rights, Report of the United Nations High Commissioner for Human Rights*, 7 August 2024, paras. 19, 20, 31.
[53] Interview with Child Protection INGO.
[54] Interview with counterterrorism expert.
[55] Interviews with two UN workers and child protection INGO.
[56] Interview with child protection INGO.
[57] Interview with UN worker.
[58] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, submitted in accordance with Assembly resolution 72/180 and Human Rights Council resolution 49/10*. A/77/345, 16 September 2022, para. 44.

.

Application of exemptions on national security grounds

A further challenge lies in the exemptions granted to national security entities. At both national and regional levels, data protection laws often carve out broad exemptions from most data protection rights and obligations when data is gathered for security or defense purposes.[59] At EU level, article 4 of the Treaty of the European Union stipulates that national security remains the sole responsibility of each Member State.[60] It is up to each country to regulate the functioning of its intelligence services, and EU data protection laws, including those applicable to law enforcement, are not applicable to intelligence services.[61] This decentralized approach has led to fragmented oversight, making it difficult to assess what data is collected, how it is used, and with whom it is shared.

In principle though, the security exemption should only be applied on a case-by-case basis, and any interference with privacy rights should be necessary and proportionate in a democratic society to meet a pressing social need.[62] So, States must apply a proportionality test to determine if the need to hold the data warrants any infringement of the right to privacy. The more intrusive the data, the higher the threshold this proportionality test must meet.[63] Yet, in practice, the threshold for justifying mass data collection appears increasingly low. Some scholars even argue that ´national security´ in Europe has become a *de facto* exemption from human rights obligations[64], as if shifting the burden of proof—where individuals must now justify why they deserve privacy, rather than the State having to justify why their data should be collected.

In addition, there is evidence of little independent oversight of data collected by security and intelligence agencies.[65] It would be worth exploring if at the national level there is any particular oversight specifically in relation to data gathered on children by these agencies.

III. Collection of children´s personal data on counterterrorism grounds

Data collection from children recruited by armed groups designated as terrorist groups

The recruitment and exploitation of boys and girls under 18 by armed groups have long been a trend in armed conflicts.[66] Armed groups, including those designated as terrorist groups, have utilized children to further their military and political objectives,[67] not just as fighters but in a wide range of other roles. For example, ISIL notoriously

[59] Examples of restrictions to rights for reasons of national security and defense: Art. 23 of the EU GDPR; UK GDPR, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/; Article 37 of the Personal Data Act 2022 of Niger, https://www.dlapiperdataprotection.com/?t=collection-and-processing&c=NE#insight; Article 13 of Data Protection Law of Burkina Faso of 30 March 2021 N°001-2021/AN; Article 17 of Data Protection Law of Mali of 21 May 2013 N°2013-015; Article 5 of Data Protection Law of Mauritania N°2017-020 of 22 July 2017.

[60] Article 4.2 of the Treaty of the European Union, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF. This exemption from EU law could be interpreted as meaning that Article 8 of the EU Charter on Fundamental Rights (CFR) and Article 16 of the Treaty on the Functioning of the European Union (TFEU) on the right to personal data protection should not apply to any national security matters governed by domestic law as these provisions are only relevant to 'Member States when carrying out activities that fall within the scope of EU law.'

[61] See Art. 2.3. a) of EU Directive 2016/680 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[62] https://ico.org.uk/for-organisations/intelligence-services-processing/exemptions/#what

[63] *Prevent and the Pre-crime State: How unaccountable data sharing is harming a generation*, Open Rights Group, February 2024.

[64] "When 'bad countries' make good caselaw: Digital surveillance technologies and the protection of privacy in the Council of Europe area" by Sophie Duroy (University of Essex) and Martin Scheinin (University of Oxford).

[65] *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, Privacy International, April 2018.

[66] Secretary General Reports on Children Affected by Armed Conflict at Library – Office of the Special Representative of the Secretary-General for Children and Armed Conflict (un.org).

[67] Committee on the Rights of the Child, General comment No. 24 (2019) on children's rights in the child justice system, para. 98.

.

deployed children in suicide attacks and combat, while also using them for domestic and logistical tasks such as cooking, transporting weapons, manning checkpoints and using girls as wives.[68] Similarly, Al-Shabaab in Somalia and Boko Haram in the Lake Chad Basin region have systematically forced children—through abduction, coercion or manipulation—into supporting their operations, with Boko Haram notably using girls as suicide bombers.[69] The cruel treatment of children by armed groups is not new. The Lord's Resistance Army (LRA) in Uganda, active over decades, abducted an estimated 20,000 children.[70] Accounts from survivors, such as one boy's harrowing story of being forced to kill a fellow child captive for attempting to escape, underscore the brutality of this group's tactics.[71]

Recognizing that these children are victims first and foremost, child protection efforts have focused on promoting and supporting their rehabilitation and reintegration. In several African countries (Burkina Faso, Central African Republic, Chad, Mali, Niger, Nigeria, Somalia, Sudan and Uganda[72]), so called "handover protocols" have been adopted. These (non-legally binding) agreements, signed between the UN and national governments, mandate the swift transfer of children allegedly associated with armed groups to civilian child protection authorities, to ensure the children get access to reintegration support instead of being detained, or left on their own.[73] The handover protocols afford equal treatment to all children exiting armed groups, regardless of whether the armed groups have been designated as terrorist.

Now, a critical question arises: what happens to the personal data of these children? While the handover protocols prohibit intelligence-gathering interrogations, they remain quite generic on the issue of identification. The protocols typically contain a standard clause which stipulates that the military or security forces can ask the children about their name, health, and family situation but should not interrogate the children to gather intelligence. Do military or security forces (who generally are the first point of contact upon the children's encounter), collect the children´s biometric data, such as fingerprints? How long can children´s personal data be stored by the military or security services? Who has access to it? And perhaps most concerning, would this information be used for counterterrorism purposes rather than just for family reunification or rehabilitation?

These questions are even more critical in conflict contexts where specific data protection laws are absent, like Iraq and Syria, or they are quite new, like Somalia or Nigeria, and implementation remains weak. Further, as a former soldier put it, in such conflict zones privacy is not a military priority.[74] This adds another layer of risk: data security. Poorly protected data can fall into the wrong hands, putting children at risk. A regime change can turn personal

---

[68] *UN Security Council, Iraq Report* (S/2019/984), paras. 29, 31, 32 and 34; *Report of the Secretary-General on children and armed conflict in Iraq*, 9 November 2015; *UNAMI/OHCHR Report on the Protection of Civilians in the Armed Conflict in Iraq: 11 December 2014-30 April 2015*; *"Maybe We Live, and Maybe We Die," Recruitment and Use of Children by Armed Groups in Syria*, Human Rights Watch 2014; "I Am Nothing Without a Weapon, Understanding Child Recruitment and Use by Armed Groups in Syria and Iraq" by Mara Revkin, in *Children and Extreme Violence: Cradled by Conflict,* United Nations University, 2018; Security Council Resolution 2349 (2017) para. 1.

[69] *No Place for Children: Child Recruitment, Forced Marriage, and Attacks on Schools in Somalia*, Human Rights Watch 2012; "*Our job is to shoot, slaughter and kill', Boko Haram's reign of terror in north-east Nigeria*, Amnesty International, April 2015; *Silent Shame: Bringing Out the Voices of Children Caught in the Lake Chad Crisis,* UN Children's Fund, 27 April 2017, p. 3.

[70] "Child combatants in Northern Uganda: Reintegration myths and realities" by Christopher Blattman and Jeannie Annan, in *Security and Post-Conflict Reconstruction: Dealing with Fighters in the Aftermath of War,* Robert Muggah, Routledge, 2008, p. 103–126.

[71] *Abducted and Abused: Renewed Conflict in Northern Uganda*, Human Rights Watch, Vol. 15, No. 12 (A), July 2003.

[72] See S/RES/2349 (2017), para. 30; *A Path to Reintegration: The Role of Handover Protocols in Protecting the Rights of Children Formerly Associated to Armed Forces and Armed Groups*, Watchlist policy note, 2020; https://upr-info.org/sites/default/files/country-document/2023-11/OSRSG_CAAC_UPR44_BFA_E_Main.pdf; https://childrenandarmedconflict.un.org/2024/10/car-important-milestone-for-the-protection-of-children-with-adoption-of-a-handover-protocol/

[73] The transfer may take place within several days or, in some cases, weeks. *Child Exits from Armed Groups in the Lake Chad Basin*, UNIDIR MEAC Findings Report 31, June 2023; *Targeted by Terrorists: child recruitment, exploitation and reintegration in Indonesia, Iraq and Nigeria*, UNODC, 2024.

[74] Interview with former army officer.

.

data into a tool for targeting specific groups. The mass collection of personal data by the U.S. in Afghanistan—later seized by the Taliban—demonstrates this danger.[75]

In the drafting of handover protocols, however, there appears to have been little or no consideration of whether children's identifying information might end up in databases held by military or security agencies, or even be shared more broadly, including overseas.

Reports indicate that in some countries, children who should be promptly transferred to civilian child protection services first undergo some sort of screening by military or security forces. In some cases, foreign military advisors assisting national forces have also been involved.[76]

This raises concerns that children´s personal data collected at the point of capture or surrender may be stored and used for broader counterterrorism purposes—especially since initial interactions with the children occur without civilian or child protection actors being present in frontline areas, and later children may not spontaneously disclose such data collection unless specifically asked.[77] These concerns suggest that handover protocols could be strengthened to include clearer rules on the handling of children's personal data.

Not all children disengaging from armed groups though are recorded or profiled by security forces, as some return directly to their communities without passing through formal (DDR) processes.[78] Also, in some conflict settings, the risk of having children's data systematically collected and processed by security forces may be minimal or speculative due to limited logistical and technical capacity for systematic and sustainable data collection. Factors like lack of electricity, high costs of biometric tools, and scarce resources in remote or insecure areas hinder such efforts. However, evidence of security-led data collection of children´s personal data in some conflict contexts, even if inconsistent, shows that the risk is not entirely absent.

Some country-specific practices of children´s personal data collection for counterterrorism purposes are detailed in Annex I.

Collection of data from children with family links to armed groups designated as terrorist

Beyond the issue of children recruited and/or exploited by terrorist-designated armed groups, children have been listed and even deprived of their liberty due to presumed familial association to these groups. A troubling trend in counterterrorism responses is the assumption that relatives of armed group members are also supporters or members themselves, which impacts disproportionately on women and children.[79] This is most evident in the mass indefinite arbitrary detention of thousands of children in inhumane conditions in camps in northeastern Syria. Children in these camps—particularly in the notorious Al-Hawl camp—are unlawfully deprived of liberty without individual legal determinations, premised on the alleged threat they pose to security, on the basis of their or their parents´ alleged prior links to ISIL/Daesh.[80] As observed by the former Special Rapporteur on

[75] "Biometric data flows and unintended consequences of counterterrorism" by Katja Lindskov Jacobsen in *International Review of the Red Cross* (2021), 103 (916-917), 619–652; "The Taliban Have Seized U.S. Military Biometrics Devices", The Intercept, 17 August 2021; *New Evidence that Biometric Data Systems Imperil Afghans,* Human Rights Watch, 30 March 2022.

[76] Interviews with former humanitarian workers in Mali and the Sahel.

[77] Interview with researcher on the Lake Chad Basin.

[78] *Child Exits from Armed Groups in the Lake Chad Basin*, UNIDIR MEAC Findings Report 31, June 2023; interviews with sources who worked in Cameroon and Nigeria.

[79] *The Limits of Punishment Transitional Justice and Violent Extremism*, United Nations University, May 2018; Interview with lawyer assisting former Guantanamo underage detainees.

[80] *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic* A/HRC/49/77 *para. 112; Technical Visit to the Northeast of the Syrian Arab Republic End of Mission Statement (*of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), para. 6.
https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/EoM-Visit-to-Syria-20230721.pdf

.

counterterrorism and human rights, Ms. Fionnuala D. Ní Aoláin, northeast Syria has become "the largest site of detention of children for counter-terrorism purposes worldwide."[81]

In the so called Annex of the Al-Hawl camp, which functions as a prison within a prison, women and children foreign nationals "are vulnerable to trafficking, sexual violence, obstetric and other forms of violence, as well as profound material deprivation."[82] Some of these women were trafficked to northeastern Syria when they were adolescent girls.[83] Adolescent boys in the camp, as young as 10, are systematically forcibly separated from their mothers and transferred to so called rehabilitation centers that amount to detention centers, and some to military detention.[84] In the Gweiran Sina'a/Panorama prison in northeastern Syria, "men and children, detained without any legal process, are subjected to incommunicado detention and disappearances and risk death from inadequate food, starvation and exposure to widespread tuberculosis without available treatment, which constitute core international crimes. These children are above all victims of terrorism" .[85]

Data collection in north-east Syria has been massive, with the US-led coalition assisting in the screening of residents who fled the last ISIL-held territories, including women and children. Amnesty International reported how the Syrian Democratic Forces (SDF) and US-led coalition kept files on every man, woman and child with perceived affiliation to ISIL held in detention facilities in north-east Syria, including their biometric data (DNA, iris scan and their fingerprints).[86] The US-led coalition reportedly separated teenager boys suspected as fighters and took their biometric data; it is not clear though where the biometric information went to.[87] More generally, the level to which children's personal data, including biometric data, is being systematically recorded and updated in camps, is unclear.[88] On data collection, "everybody is in the dark in Al-Hawl camp", a journalist said.[89]

Organized repatriation operations from Al-Hawl camp involving women and children who are third-country nationals have largely been facilitated by the U.S.[90], suggesting that the personal data of these children has likely been collected by the U.S. during the process.[91] Upon children´s return to their home countries (unaccompanied or with their mothers), national law enforcement and security agencies are typically involved to some extent in

---

[81] A/78/520, October 2023.

[82] *Visit to Bosnia and Herzegovina Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism, Fionnuala Ní Aoláin*, A/HRC/55/48/Add.1, 11 March 2024, para. 32.

[83] Communication by NGO Reprieve.

[84] *Report of the Independent International Commission of Inquiry on the Syrian Arab Republic* A/HRC/51/45, para. 98; *End of mission statement, Visit to the Syrian Arab Republic – Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, para. 15; Interviews with Professor Harmonie Toros, journalist Anand Gopal and NGO worker in Al Hawl camp; https://news.un.org/en/story/2023/07/1138972. At the rehabilitation centres there are children accused of association with ISIL but who were not involved in attacks (e.g., used as cleaners, spies or supporters): Interview with UN worker. See case of French boys aged 12 separated from their mothers in Al-Hawl and Al-Roj camps to be placed in Orkech and Houry "rehabilitation centers": https://www.famillesunies.fr/

[85] *Visit to Bosnia and Herzegovina Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism, Fionnuala Ní Aoláin*, A/HRC/55/48/Add.1, 11 March 2024.

[86] *Aftermath, injustice, torture and death in detention in North-east Syria*, Amnesty International, 2024, p. 52. See also *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin*, A/78/520, para. 60. "Scrambling to Track Islamic State Terrorists, Coalition Turns to Biometrics", VOA News, November 2017 at https://www.voanews.com/a/track-islamic-state-terrorists-biometrics/4106535.html

[87] Discussion with Amnesty International. See also *Aftermath, injustice, torture and death in detention in North-east Syria*, Amnesty International, 2024, p. 57.

[88] Interviews with Professor Harmonie Toros, NGO worker in Al Hawl camp, journalist, and lawyer involved in security detention case in Syria.

[89] Interview with Anand Gopal.

[90] For example, repatriation efforts with U.S. support in 2023 included the Kyrgyz Republic's repatriation of 333 displaced persons (97 women and 236 children) in four separate repatriation operations and Iraq's conducting nine repatriation operations of nearly 300 fighters and more than 3,800 family members. See *U.S. Department of State Country Reports on Terrorism 2023*.

[91] https://globalnews.ca/news/7066684/canadians-at-camp-for-isis-registration-drive/

.

reception and follow-up, which would entail a level of access to children's personal data.[92] However, countries differ significantly in how they approach reintegration, and data handling. In Sweden, for instance, repatriated children have not been prosecuted, and their files are reportedly managed by social services in the same way as any other child protection cases, although police are still involved in initial reception.[93] Notably, Uzbekistan and Kazakhstan have issued new birth certificates to returning children that omit their place of birth. This aims to shield children from automatic association with ISIL and prevent lifelong stigmatization.[94] Such practice shows that even in countries where security agencies are dominant, more sensitive treatment of children's data is possible. In some cases, returnee children have also been given new names[95] to protect them from media attention, stigma, or potential harm if identified—though this practice has reportedly led at times to confusion or identity adaptation challenges for the children involved.[96]

The case of France is of special concern regarding children´s data collection. French children repatriated to France from detention camps and facilities in north-east Syria and Iraq, depending on their age, may face prosecution if they are suspected of having participated in terrorist acts.[97] Children not believed to have participated in terrorist activities have been separated from their mothers upon arrival and placed in institutions or "with family members who do not pose a threat of radicalization to violence" and take part in a rehabilitation and reintegration program.[98] As for their personal data, Decree No. 2023-255 adopted in 2023 establishes the collection, and sharing among various State agencies, of every child returnee´s personal and biographic data until they turn 18 years.[99] The decree specifically stipulates which children´s data shall be collected, as well as an exhaustive list of the authorities (at least 10) which can have access to such data, including the police.[100]

The potential for children's data to be shared across international security networks adds another layer of complexity. While intelligence-sharing is core to international security cooperation, should children who are not responsible for their parents' choices be included in such data flows? If these children's biometric and personal data remained embedded in global counterterrorism databases indefinitely, what impact might this have on their ability to reintegrate into society, travel freely, or even access certain rights in the future?

This issue of sharing children´s personal data for counterterrorism purposes is further discussed below.

IV. Sharing of children´s personal data

The practice of sharing personal data—especially biographic and biometric data—across borders has become a cornerstone of contemporary counterterrorism strategies. Promoted vigorously by the United Nations[101] and

[92] Interview with advisor working on repatriations from Syria to Sweden.
[93] Interviews with NGO worker and with advisor on repatriations to Sweden from Syria.
[94] Discussion with UN official.
[95] Interview with advisor working on repatriations to Sweden from Syria.
[96] *Reintegration of Children Affected by Conflict in Syria to Western Europe: Lessons and Reflections Shared by Social Workers and Front-Line Service Providers*, UNICEF, September 2024.
[97] According to data from the PNAT (Parquet National Anti terroriste), as of September 2024, 364 children had returned to France.
[98] *EU Terrorism Situation and Trend Report* (TE-SAT) 2022.
[99] Décret No. 2023-255 of 6 April 2023 "autorisant la création d'un traitement automatisé de données à caractère personnel relatif à la prise en charge des mineurs de retour de zones d'opérations de groupements terroristes (MRZOGT) ».
[100] *Ibid.* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047416587
[101] Particularly Security Council Resolution 2322 (2016) requests Member States to share biometric and biographic information about foreign terrorist fighters and other individual terrorists and terrorist organizations. The UN Security Council *Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum* states: "States are encouraged to ensure the interoperability of their national watch lists and databases and to establish connectivity with regional and international watch lists and databases and enable information-sharing, as appropriate, with relevant competent authorities, whether nationally or internationally".

.

implemented at national, regional, and international levels,[102] such data exchanges are often framed as essential to global security. Yet this raises pressing questions: Whose data is being shared, and under what conditions? And crucially, what happens when this data belongs to children?

The UN Security Council has issued a series of resolutions (2178 (2014), 2396 (2017), 2482 (2019) and notably 2322 (2016)) that not only encourage, but effectively require, States to improve cooperation in preventing the movement of foreign terrorist fighters. One of the key tools in this effort is the sharing of personal information of travelers —including biometric data—with international bodies such as INTERPOL.[103] UN Security Council 2396 expressly requests Member States to contribute to INTERPOL's databases and ensure that law enforcement, border security and customs agencies use INTERPOL databases in screening travelers at air, land and sea ports of entry and to strengthen investigations and risk assessments of returning and relocating foreign terrorist fighters and their families.[104] The term "families" in some provisions of the resolution expressly refer to both the spouses and the children of foreign terrorist fighters.[105]

One example of this drive is the UN Counter Terrorist Travel Programme and the goTravel Software Solution. While its main objective—to help States use Advance Passenger Information (API) and Passenger Name Records (PNR)[106]—is framed in terms of enhancing security, serious concerns arise. The program's opacity, combined with the broad powers granted to national border authorities, raises the question of oversight to prevent misuse, from discriminatory profiling to unjust surveillance.[107] Basically, who is watching the watchers?

Within the EU, data sharing is not only permitted—it is being structurally integrated through the interoperability of security and migration databases.[108] EU-LISA (the European Union Agency for the Operational Management of

---

[102] For instance, the *Joint Action Plan on Counter-Terrorism for the Western Balkans*, supported by the EU, expressly requires the concerned states to "boost spontaneous Counter-Terrorism related information exchange on bilateral and multilateral level within the Western Balkans region, with Europol's European Counter-Terrorism Centre, EU Member States and Europol's operational partners using secure channels such as SIENA/CT SIENA; exchange information with Interpol Counter-Terrorism relevant databases (notably on Foreign Terrorist Fighters)…to tackle the travel of the known/listed Foreign Terrorist Fighters on the way to or from conflict zones". Russia, Iraq, Iran and Syria have formed an intelligence sharing arrangement to facilitate cooperation in combating the Islamic State. One of the best known sharing arrangements is the Five Eyes alliance between the US, UK, Australia, Canada and New Zealand. See *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, Privacy International, April 2018. Judgments on renditions show there was extensive sharing of data across the UK, U.S., Poland, Lithuania, Thailand, the Maghreb, Syria and Libya. Interview with human rights worker involved in advocacy around rendition programmes.

[103] Resolution 2396 (2017), para. 15: "*Decides that* Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law… and *encourages* Member States to share this data responsibly among relevant Member States, as appropriate, and with INTERPOL and other relevant international bodies".

[104] Resolution 2396 (2017), para. 16.

[105] Resolution 2396, paras. 29 and 30. See also Resolution adopted by the General Assembly on 22 June 2023 The United Nations Global Counter-Terrorism Strategy: eighth review A/RES/77/298, para. 53.

[106] The program helps states to screen travelers and cross-check them against INTERPOL, and other international and national databases of known and suspected terrorists and criminals, in accordance with Security Council resolutions. See https://www.iom.int/news/iom-and-unoct-sign-agreement-collaborate-api/pnr-technical-assistance; Security Council Resolution 2178.

[107] UN Countering Terrorist Travel Programme, https://www.un.org/cttravel. *Position Paper of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism Fionnuala NíAoláin on the United Nations Countering Terrorist Travel ("CT Travel") Programme and the goTravel Software Solution*, 30 October 2023, at https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/2023 -10-30-a-ct-travel-gotravel-position-paper.pdf; *Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space* by Annabelle Bonnefont, Global Center on Cooperative Security, March 2024, p. 16.

[108] At least these three information systems can be connected: the Schengen Information System (SIS) which contains a broad spectrum of alerts on persons (refusals of entry or stay, EU arrest warrants, missing persons, judicial procedure assistance, discreet checks); the Eurodac system with fingerprint data of asylum applicants and of third-country nationals who have crossed the external borders

.

Large-Scale IT Systems in the Area of Freedom, Security and Justice) plays a central role in enabling the exchange of personal data, including biometric data, across various large-scale IT systems. The stated aim is efficiency—making all systems "work together as one".[109]

In this context, a pivotal question emerges: Is data about children formerly or allegedly associated with armed groups designated as terrorist, or even children linked to such groups by family ties, being shared across borders and into security databases? The answer is elusive. Data sharing agreements tied to law enforcement and intelligence, are typically confidential.[110] But the absence of clear exclusions for children in the public versions of certain such agreements (for example, the EU–U.S. data sharing related agreement) suggests that, in practice, children´s data may well be included.[111] This raises troubling possibilities. Children first and foremost victims of exploitation by terrorist-designated armed groups could find themselves listed, monitored, or even denied asylum abroad, as well as on the basis of family ties or erroneous associations.

This situation is heightened by a general lack of transparency, accountability and oversight of intelligence-sharing arrangements,[112] and (with a few exceptions) a general lack of compliance of intelligence-sharing with the principle of legality under international human rights law.[113]

Further, while many data protection frameworks, particularly the EU General Data Protection Regulation (GDPR), require data protection "adequacy" or equivalent protections in third countries to which data is transferred, these explicit standards appear to be one-sided: they apply to outgoing data, not incoming. This EU rule of equal data protection standards not only applies to data sharing for commercial purposes, as in the GDPR, but also to data sharing for law enforcement purposes.[114] EUROPOL, for instance, must check the data protection standards of

---

irregularly or who are irregularly staying in a Member State; and the Visa Information System (VIS) with data on short-stay visa holders. See https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_5241

[109] https://www.eulisa.europa.eu/activities/interoperability. EU Lisa connects EU criminal records of third country nationals, EES (entry/exit system) and ETIAS which are about to start fucntioning, visa information systems, and the EU travel information authorization system, ETIAS. The Schengen Information System is linked to the system as well, although not part of it. These systems are used for checks at border crossings; the data is connected to multiple identity detectors. Interview with Yasha Maccanico from Statewatch. See https://www.statewatch.org/media/3143/building-the-biometric-state-police-powers-and-discrimination.pdf

[110] "Biometric data flows and unintended consequences of counterterrorism" by Katja Lindskov Jacobsen in *International Review of the Red Cross* (2021), 103 (916-917), 619–652. Interview with data protection expert; *Human Rights Implications of the Use of New and Emerging Technologies in the National Security Space* by Annabelle Bonnefont, Global Center on Cooperative Security, March 2024.

[111] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, 10 December 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22016A1210%2801%29; Agreement on mutual legal assistance between the European Union and the United States of America (Art.9

[112] A/69/397, para. 44; CCPR/C/GBR/CO/7, para. 24; CCPR/C/SWE/CO/7, para. 36.

[113] *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards*, Privacy International, April 2018. Special Rapporteurs on human rights and counterterrorism have consistently recommended that States must be obliged to provide a legal basis for the reuse of personal information, in accordance with human rights principles, especially where information is shared across borders or between States. See A/HRC/13/37, paras. 50 and 66. The Council of Europe Commissioner for Human Rights has recommended that intelligence oversight bodies be mandated to scrutinize the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information. See www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

[113] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson*, A/69/397, 23 September 2014.

[114] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Articles 44-46; Recital 67: "In line with the fundamental values on which the Union is founded, in particular the protection of human rights, the Commission should, in its assessment of the third country, or of a territory or specified sector within a third country, take into account how a particular third country respects the rule of law, access to justice as well as international human rights norms and

.

countries with which it shares personal data.[115] Yet, the above adequacy requirement refers to transferring data, not to receiving data,[116] and does not explicitly refer to due diligence on human rights´ compliance by third (non-EU) countries from where the data is received. In fact, intelligence services frequently receive data from countries with weak or non-existent human rights protections—often without investigating how that data was gathered.[117] Some legal frameworks even explicitly permit this kind of selective scrutiny in the name of counterterrorism.[118]

So, what happens when the data being shared pertains to children—possibly detained, convicted, or merely listed in countries where due process is weak or absent? Or based on unreliable data, solely on family links to a terrorist group, or on a too broad interpretation of "association" with an armed group? In countries like Iraq, for instance, children have been detained or blacklisted solely because of their relatives' alleged involvement with terrorist groups, or even due to mistakes in security lists, such as similar or misspelled names.[119] And where accountability mechanisms are virtually non-existent, how can a child—or their guardians—possibly challenge these actions or seek justice?

Another murky area involves intra-State data sharing. For example, it remains unclear to what extent data from "deradicalization" or Preventing or Countering Violent Extremism (PVE/CVE) programs—some of which are run by NGOs or local authorities—is shared with national security agencies.[120]

Interoperability: Enhancing security or eroding privacy?

Interoperability, for the purposes of this paper, refers to the ability of information systems to exchange data. In the United States, for instance, the consolidated Terrorist Screening Database (TSDB) is made available widely—

---

standards and its general and sectoral law, including legislation concerning public security, defense and national security, as well as public order and criminal law. The adoption of an adequacy decision regarding a territory or a specified sector in a third country should take into account clear and objective criteria, such as specific processing activities and the scope of applicable legal standards and legislation in force in the third country. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and –judicial redress". Transfers not based on such an adequacy decision should be allowed only where appropriate safeguards have been provided in a legally binding instrument which ensures the protection of personal data or where the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist."

[115] Interview with security agency and data protection experts. The amendment of Regulation (EU) 2016/794 by Regulation (EU) 2022/991 introduced provisions that allow Europol to receive personal data from third countries without an operational agreement, provided certain data protection safeguards are in place. See https://eur-lex.europa.eu/eli/reg/2022/991/oj

[116] However, Article 5 of the GDPR provides as a general principle that data must be accurate and be kept updated.

[117] See for instance reports on secret detentions and renditions in third countries as part of the U.S. Global war on terror. *Secret detentions and illegal transfers of detainees involving Council of Europe member states: second report,* Rapporteur Mr. Dick Marty, Council of Europe Committee on Legal Affairs and Human Rights, 7 June 2007.

[118] For example, Argentinian Law on the protection of personal data: "Article 12 -- International transfer:
1. The transfer of personal data of any kind to countries or international or supranational organizations that do not provide adequate levels of protection is prohibited.
2. The prohibition shall not apply in the following cases:
…e) When the transfer is intended for international cooperation between intelligence agencies to combat organized crime, terrorism and drug trafficking".

[119] *Everyone Needs to Confess" Abuses against Children Suspected of ISIS Affiliation in Iraq*, Human Rights Watch 2019. Perceived affiliation currently takes many forms, though the most common is through a familial connection (e.g., through a parent or sibling who was actively involved with ISIS). See "Distinguishing Children From ISIS-Affiliated Families in Iraq and Their Unique Barriers for Rehabilitation and Reintegration" by Joana Cook in *Perspectives on Terrorism* Volume XVII, Issue 3, September 2023.

[120] Interview with counterterrorism expert.

.

not just to federal agencies, but to local authorities, private entities, and foreign governments that have entered into immigration agreements with the U.S. or that are engaged as U.S. partners to fight terrorism.[121]
The move toward interoperability of systems across borders reinforces the need to examine data sharing critically.

In Europe, EURODAC (the European Asylum Dactyloscopy Database)— a fingerprint database originally established for asylum and migration management—has expanded to allow law enforcement access. The European Data Protection Supervisor (EDPS) expressed concern at this expansion granting law enforcement authorities access to data of individuals in principle not suspected of committing any crime. It also highlighted the vulnerability of asylum seekers and questioned the necessity of granting security agencies access to data collected for entirely different purposes.[122] The EDPS stressed the need for clear justification and compliance with necessity and proportionality tests, including proof that less intrusive means were unavailable to achieve the envisaged security purpose. Currently, agencies like EUROPOL can access EURODAC and request biometric data comparisons, "including to respond to the threat from radicalized persons or terrorists who might have been registered in EURODAC".[123]

Also, INTERPOL, EUROPOL, and national security entities maintain vast databases of suspected terrorists—often populated through international data sharing.[124] INTERPOL operates 19 databases, some of which support counterterrorism efforts.[125] At the European level, the Schengen Information System (SIS) is the largest security and border management information sharing system. It allows border, immigration, police, customs, and judicial authorities across the EU to access shared "alerts" on individuals.[126] Since July 2022, EUROPOL can propose that EU countries enter alerts into the SIS based on information received from non-EU States and international organizations.[127] As a result, individuals—potentially including children—placed on watchlists by non-EU States and international entities could be added to the Schengen database via EUROPOL.

With the 2024 European Pact on Migration and Asylum now mandating biometric data collection and security screening at EU borders of all third-country nationals—including children—who meet certain conditions, the implications become even more acute.[128] Third-country nationals shall "undergo a security check to verify whether they might pose a threat to internal security", and to this end, the Schengen Information System, EUROPOL and

---

[121] *CRS Report for Congress Terrorist Identification, Screening, and Tracking Under Homeland Security Presidential Directive 6* April 21, 2004.
[122] EDPS Opinion 2010/C 92/01.
[123] 2024 EURODAC Regulation, Recital 28: "In the fight against terrorist offences and other serious criminal offences, it is essential for law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in Eurodac is necessary for the purposes of the prevention, detection or investigation of terrorist offences as referred to in Directive (EU) 2017/541 or of other serious criminal offences as referred to in Framework Decision 2002/584/JHA. Therefore, the data in Eurodac should be available, subject to the conditions set out in this Regulation, for comparison by Member States' designated authorities and the designated authority of the European Union Agency for Law Enforcement Cooperation (Europol)…" See also Recitals 35 and 36.
[124] *U.S. Department of State Country Reports on Terrorism 2022.*
[125] https://www.interpol.int/en/How-we-work/Databases/Our-19-databases
[126] https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en
[127]https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en. See Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation. In line with this Regulation, EUROPOL may propose the possible entry by the Member States, at their discretion and subject to their verification and analysis of those data (data provided by third countries or international organizations to Europol on persons involved in terrorism or in serious crime), of information alerts on third-country nationals in the interest of the Union ("information alerts") in the Schengen Information System (SIS). See https://www.statewatch.org/news/2022/november/new-europol-rules-massively-expand-police-powers-and-reduce-rights-protections/.
[128] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1356

.

INTERPOL databases, among others, shall be consulted.[129] If the consultation with security databases results in a "hit" (match), this will not be explained but "will be redacted in the information contained in the form that shall be made available to the person concerned".[130] So, a child flagged in INTERPOL or EUROPOL databases, potentially due to family links to a terrorist group or to a foreign terrorist fighter, may be denied protection without even being informed of the reasons why.

It is also worth examining how the Africa-Frontex Intelligence Community (AFIC) eventually handles personal data sharing, particularly concerning children. AFIC is a network of 30 African states cooperating with Frontex (the European Border and Coast Guard Agency), on risk analysis to combat cross-border crime and terrorism.[131] Frontex states that information shared within AFIC contains no personal data and excludes national intelligence service data. However, concerns have been raised that some African border authorities cooperating with Frontex may, in practice, possess actual powers akin to intelligence services.[132]

Beyond government and intelligence actors, humanitarian agencies also collect personal data, including of children. Large agencies have established institutional personal data protection policies which include limitations to the transfer and retention of beneficiaries´ personal data.[133] Yet, smaller NGOs, particularly those reliant on funding for CVE (Countering Violent Extremism), may face pressures to share data with authorities wishing to use such data for other purposes, such as control of migration flows and the fight against terrorism.[134] As a 2015 Privacy and Data Protection Commissioners´ resolution warned, such risk is very real and could undermine both the safety of beneficiaries, such as displaced persons, and humanitarian action more broadly.[135]

This humanitarian dimension, while beyond the scope of this paper, points to a wider concern: the expanding practice and risks of data collection and sharing,[136] and the shrinking space for oversight.

Watch Listing: A shadow system

At the heart of data-sharing practice lies the system of watch listing. Watch listing lacks consistency and predictability. First, States apply no universal standards or criteria for adding individuals to terrorist watch lists, for managing or sharing these databases, or establishing procedures for removal.[137] Also, individuals often don't know

---

[129] Articles 15 and 16 of the Regulation (EU) 2024/1356 of the European Parliament and of the Council of 14 May 2024 introducing the screening of third-country nationals at the external borders and amending Regulations (EC) No 767/2008, (EU) 2017/2226, (EU) 2018/1240 and (EU) 2019/817.

[130] *Ibid*, Article 17.3.

[131] AFIC was launched in 2010 to promote regular information exchange on migrant smuggling and other border security threats affecting African countries and the EU. EU Frontex funded a project to train and equip local border police analysts in eight western African countries to collect and analyze data on cross-border crime and support authorities involved in border management. https://www.frontex.europa.eu/media-centre/news/news-release/eight-afic-risk-analysis-cells-set-a-benchmark-in-africa-uwxHJU

[132] https://www.statewatch.org/media/3485/ep-frontex-afic-answer01.pdf

[133] For instance, UNICEF and ICRC data protection policies: https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf; https://shop.icrc.org/icrc-rules-on-personal-data-protection-print-en.html

[134] For instance, humanitarian agencies were requested by USAID to report whether recipients of aid may be linked to terrorist groups, to ensure that USAID funds are not diverted to support terrorist activities. See USAID antiterrorism contractual clauses in grants and cooperative agreements, ADS Chapter 303.

[135] The Resolution on Privacy and International Humanitarian Action issued in 2015 at the 37th International Conference of Privacy and Data Protection Commissioners states that "humanitarian organizations not benefiting from Privileges and Immunities may come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism). The risk of misuse of data may have a serious impact on data protection rights of displaced persons and can be a detriment to their safety, as well as to humanitarian action more generally." See https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf

[136] https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

[137] *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum*, S/2015/939 and S/2018/1177.

.

they have been listed[138]—intelligence-based lists are not public—and clearing one's name in one jurisdiction doesn't guarantee deletion elsewhere. Persons listed may be unable to remove themselves from the multiple lists that have emerged since then. Once a list is shared internationally, individuals often cannot trace the source of the information, understand why they were first listed, or challenge foreign authorities' conclusions, and may be denied the opportunity to exercise rights in domestic courts.[139] Additionally, when data from multiple sources is combined, algorithms can wrongly flag innocent people as threats.[140]

The concerns with watch listing are hence many: Lack of transparency, vague or minimal evidentiary standards in placement;[141] unpredictable data replication across systems; and limited avenues for review or removal.

For example, a U.S. Government policy is to refuse to confirm or deny an individual's watch list status or provide the factual basis for inclusion.[142] Under U.S. watch listing guidance, non-U.S. citizens may be listed based on a "possible nexus to terrorism," even when supporting information is very limited or of suspected reliability or based solely on association with someone already listed. As the American Civil Liberties Union (ACLU) notes, an "unfortunate acquaintance may be all it takes to deny someone U.S. citizenship or permanent residence in the United States."[143] Most people on the U.S. Terrorist Screening Database are, in fact, foreigners.[144]

Children are not spared. U.S. policy, for instance, stipulates that **children of a known or suspected alien terrorist will be included in the Terrorist dataset until they turn 21 years**, by the mere fact of the family link.[145]

---

[138] Individuals are added to the U.S. No Fly List at the government's discretion, with almost no transparency as to when or why it occurs. The process for removing individuals from the No Fly List is just as opaque and discretionary as the process for placement on the List. See *Brief for the American Civil Liberties Union and the ACLU Foundation of Oregon as Amicus Curiae supporting respondent in FBI v Yonas Fikre,* at https://assets.aclu.org/live/uploads/2023/12/Federal-Bureau-of-Investigation-et-al-v-Yonas-Fikre-ACLU-AMICUS-BRIEF.pdf

[139] For instance, a person with no connection to the U.S. would have no constitutional rights under the U.S. law to challenge being on a U.S. watch list and may have a weaker case under domestic law. Discussion with Professor Jeffrey Kahn.

[140] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009, para. 37.

[141] https://www.nbcnews.com/politics/national-security/terror-watchlists-too-broad-may-violate-travelers-rights-rcna130358

[142] *USA 2013 Watch listing Guidance,* at section IV Watch listing policies, Art. 1.21. https://www.justsecurity.org/66105/elhady-kable-what-happens-next-why-a-judges-terrorism-watchlist-ruling-is-a-game-changer/; https://www.justsecurity.org/wp-content/uploads/2019/09/watchlist-decision-elhady-sept-4-2019.pdf

[143] https://www.aclu.org/news/national-security/governments-own-rules-show-why-watchlists-make-bad; https://www.aclu.org/documents/whats-wrong-governments-rules-watchlisting. Reportedly, U.S. citizens and non-citizens can be watch listed based on information that hasn't been verified, or for knowing someone already on the watch list.

[144] In a 2008 hearing the FBI's Terrorist Screening Center testified that the Terrorist Screening Database was updated daily and contained approximately 1 million records relating to 400,000 individuals, of whom only 3% were U.S. persons (i.e., U.S. citizens and lawful permanent residents). See https://en.wikipedia.org/wiki/Terrorist_Screening_Database

[145] *USA 2013 Watch listing Guidance*, at 3.14.1 "An alien spouse or child of an alien who is believed to be inadmissible under the INA for terrorist activities should be nominated. No additional DEROGATORY INFORMATION (in addition to familial relation) is required for nomination under this section, if the individual meets the below qualifications.

"3.14.1.1:"To qualify for watch listing, alien spouses and children of a KNOWN or SUSPECTED TERRORIST must:

3.14.1.1 .1 Be an alien (not a U.S. citizen or national), which includes LPRs; and,

3 .14.1.1 .2 **Be an unmarried child under the age of 21 or a spouse of an alien.**

3.14.1.3 Once a spouse or child no longer meets the definitional requirements under this section, such an individual should no longer be watch listed unless there is a REASONABLE SUSPICION to believe that the individual is engaging in TERRORISM and/or TERRORIST ACTIVITIES. For example, if a child reaches the age of 2l and there is REASONABLE SUSPICION to believe he or she was knowingly involved in TERRORIST ACTIVITY by providing material support to a FTO, he or she can remain watch listed based upon this DEROGATORY INFORMATION. On the other hand, once a child of a KNOWN or SUSPECTED TERRORIST turns 21 years of age, the individual should no longer be watch listed under this exception because he or she is not considered a child of the KNOWN or SUSPECTED TERRORIST and additional DEROGATORY INFORMATION would be needed to meet the REASONABLE SUSPICION". See https://archive.org/details/Terrorism-Watchlist-Guidance-2013.

.

At the same time, children often have even fewer means than adults to challenge such listings or understand their implications.

There is, at least, growing recognition of the risks entailed for children. Acknowledging that persons under 18 may be included in watch lists, the Global Counterterrorism Forum has recommended taking into account the effects watch listing can have on children, and to set specific and distinct regulatory frameworks regarding their inclusion in watchlists, which should take into account the children´s best interests.[146] More decisively, the UN Secretary-General has called for a **complete exclusion of children from watch lists based on family affiliation or alleged affiliation with an armed group,** unless there is clear criminal evidence.[147]

This recommendation echoes a broader concern: current practices appear to prioritize suspicion over due process. And at what cost to the rights of children?

V. Harm - Consequences on children

Thousands of children are detained on national security grounds—often not for crimes they committed, but because they were unlawfully recruited by terrorist-designated armed groups, lived in territory controlled by such groups, or have family ties to them. Many are detained in conditions that expose them to inhuman treatment, torture, or even the death penalty, in clear violation of their rights to life and protection from violence. Beyond the serious concerns over the legality of these detentions and other human rights violations involved, there are also long-term risks tied to the collection of children's data during detention, and their inclusion in security databases as former detainees or convicts.[148]

Even when child justice systems allow for records to be expunged, many children formerly detained on security grounds may remain indefinitely listed in counterterrorism databases. What are the implications of such data retention for a child's future, especially when these records could travel across information systems and borders? The consequences can extend far beyond the immediate implications of detention or surveillance. In many cases, these consequences affect nearly every aspect of life, often invisibly and indefinitely. It is important to consider whether the consequences could be long-term or lifelong, because once the child reaches adulthood, if they are still on a watch list, they may no longer receive the protections granted to children.[149]

As all human rights are interrelated and indivisible, impacts on one right have implications on the enjoyment of other rights. The right to privacy, in particular, is "a gateway right", enabling and supporting a range of other rights,[150] including equality and non-discrimination, liberty, family life, free expression, assembly, and religion. Restrictions on privacy can also hinder free movement, the right to seek asylum, and access to economic and social rights such as education, employment[151] and social benefits. In this regard, former Special Rapporteur Fionnuala Ní Aoláin, indicated that families (including children) "have been subjected to listing due to their presence in

---

[146] *The Counterterrorism Watchlisting Toolkit, Global Counterterrorism Forum Watch listing Guidance Manual*, October 2021. The U.S. has trained State officials from different countries on watch listing, as part of the above "Watch listing Toolkit initiative". *U.S. Department of State Country Reports on Terrorism 2023.*

[147] *Key principles for the protection, repatriation, prosecution, rehabilitation and reintegration of women and children with links to United Nations listed terrorist groups*, UN Secretary General, April 2019.

[148] Interview with non-profit organization working in MENA region.

[149] Discussion with Professor Jonathan Todres.

[150] *Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin*, A/HRC/46/36, 22 January 2021.

[151] *U.S. Government Watch listing: Unfair Process and Devastating Consequences*, American Civil Liberties Union, March 2014.

.

conflict zones where terrorist groups are active and also experienced harsh administrative sanctions including the revocation or cancellation of social welfare benefits due to alleged affiliation with sanctioned individuals."[152]

Placing children´s data in security databases hence potentially harms their life chances, often based on a presumed risk even if the child never committed or will commit any crime. The consequences can be as significant as for criminal law, but the protections are lesser. Criminal justice systems generally require stringent evidentiary standards: the right to contest evidence, the presumption of innocence, and proof beyond reasonable doubt. If the child is found to have committed an offence and is sentenced, an assessment of the reoffending risk is made for rehabilitation purposes. In contrast, watch listing often relies on a presumed risk, sometimes merely based on a child's family ties[153] or past exploitation by armed groups. And for how long would such risk be assumed?

This raises another key question: If criminal justice systems recognize that children who have actually committed offenses can be rehabilitated with appropriate support, why should children who have not committed an offense be marked as security risks for a long (or indefinite) time? Empirical evidence suggests that children can turn away from criminal behavior swiftly and effectively when given the necessary support.[154] Long-term retention of their data, based solely on an assumed risk, seems to contradict this understanding.

The real or perceived interoperability of databases adds another layer of complexity. Could the fear of being placed on a watch list discourage children from seeking humanitarian aid, thereby restricting some of their fundamental rights, such as their access to healthcare, or social services?

Right to privacy

As described above, a crucial issue in watch listing practices is the lack of transparency. The secrecy surrounding lists such as the "No-Fly" list means individuals may be monitored without their knowledge, and with no effective oversight mechanisms. This opacity raises serious concerns about arbitrary interference with the right to privacy.[155]

A case heard before the UK High Court in 2020 illustrates the long-term impact on a child of such interference: a 16-year-old boy was found to have remained on a counterterrorism program's records for six years, despite authorities determining years earlier that he posed no risk. The police intended to retain data on the child for 6 years alleging that "radicalization is considered to be a process that occurs over time". The court ruled that retaining his data constituted a disproportionate interference with the boy´s right to privacy. It stated that although the data was not to be made public, "retention alone means that the data can be accessed by MPS (Metropolitan Police Service) officers, counter-terrorism officers nationally, local authorities and Home Office colleagues, across 10 databases…". In addition, as long as the boy´s personal data was retained, he would continue to fear that it may be disclosed to third parties, particularly universities to which he may apply or from which he may receive offers, and that he may be tagged (wrongly) as a supporter of terrorism.[156]

Some States argue, however, that sharing children's data across multiple agencies supports their rehabilitation and reintegration. For instance, France's Decree No. 2023-255 requires various State agencies to exchange personal

---

[152] *Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family*, 22 January 2021, A/HRC/46/36, paras. 20-21.

[153] https://www.justsecurity.org/79994/looks-are-deceiving-the-rebranding-and-perpetuation-of-counterterrorism-watchlisting-in-multilateral-spaces/

[154] Interview with Basile de Bure, author of *Que le destin bascule*, Ed. Flammarion, Paris, 2022.

[155] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009.

[156] Case No: CO/2962/2020 In the High Court of Justice Queen's Bench Division Administrative Court Royal Courts of Justice, 24/09/2020 at https://dpglaw.co.uk/wp-content/uploads/2020/09/2951202-R-II-v-Commissioner-of-Police-of-Metropolis-2020-EWHC-2528-Adminfinal-judgment.pdf.

.

data on children repatriated from Syria and Iraq. While officials claim this enhances coordination,[157] critics—including NGOs and families—argue it violates the right to privacy and undermines the children's best interests. Why should returnee children be subjected to a separate data system? Treating them differently from other vulnerable children within the child protection system, they argue, is itself stigmatizing. It is also reportedly unclear whether these children have been adequately informed about the collection, retention, and sharing of their data.[158] The *Conseil d'État* (the highest level of administrative jurisdiction in France) upheld the decree, ruling that data retention and interagency sharing until the returnee children turn 18 improves case tracking and coordination. It argued that the children´s judge´s decisions requiring various administrative interventions were grounded in the children´s best interests, aimed at addressing the children´s medical, psychological, academic, and administrative needs, and at preventing them "from getting involved in a process of delinquency or radicalization."[159]

Similar approaches exist in other countries. In the Netherlands, a 2017 agreement allows professionals from different sectors—including, police, prosecution authorities, courts, probation, detention facilities, families, schools and social services—to share confidential information on children as a person-specific approach to prevention of "radicalization". In Belgium, repatriated children over the age of 12 are reportedly placed on Foreign Terrorist Fighters lists and discussed in multi-agency platforms. "The goal of the approach is to provide follow-up (mostly social preventive) and to take measures to ensure their reintegration".[160] In this sense, a lawyer assisting children repatriated to a European country from Syria explained that if you don't share information the system multiplies the control over the children. "If you come back from Syria and you are a child, you get questions from the police, a doctor at the hospital, then a second or third doctor through referrals at the hospital, from the teacher, the local social services, a psychologist, the youth judge, then a different service tasked by the judge…And if you move to another county or city all this process starts all over again. Because this matter is sensitive everyone feels they need to know everything and ask everything."[161]

Enhanced coordination is a valid objective of data sharing amongst different State agencies. The challenge seems to be one of balance: How can States optimize collaboration and sharing of needed information[162] without violating children's right to privacy and not override the children´s best interests?

Freedom of movement

Increasingly, watch lists appear to breach one of the core principles of data protection: purpose limitation. This means that information collected for one specific reason may be repurposed for entirely different objectives and shared between institutions without the individual's knowledge or consent.[163] What if that information is flawed or taken out of context or based on speculation rather than substantiated facts? The consequences are far from

---

[157] The French Government has argued that sharing the returnee children´s data among State agencies is essential to enable effective coordination by the "cellule départementale de suivi pour la prévention de la radicalisation et l'accompagnement des familles" (CPRAF). See https://www.dgsi.interieur.gouv.fr/mineurs-de-retour-de-zone-syro-irakienne. This body coordinates the interventions of the relevant prefectures, health and education authorities, the director of the judicial protection of young people ("protection judiciaire de la jeunesse") and the administration of detention facilities. Such coordination arguably required access to the children´s files. Interview with French national committee for UNICEF.

[158] Interview with advocacy officer at the French national committee for UNICEF.

[159] Conseil d´Etat N°s 474251 Ligue des Droits de L'Homme (LDH), 474841 Conseil National des Barreaux (CNB), 474908 M. E...10ème et 9ème chambres réunies, Decision of 8 July 2024. https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2024-07-08/474251.

[160] *Repatriated foreign terrorist fighters and their families: European experiences & lessons for P/CVE* by Anita Perešin & Daniela Pisoiu, Radicalization Awareness Network (RAN), 2021.

[161] Interview with lawyer.

[162] *Children, the Justice System, Violent Extremism and Terrorism: An overview of law, policy and practice in six European countries* published by the International Juvenile Justice Observatory (IJJO), October 2018.

[163] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009.

.

theoretical. Individuals may be denied visas, barred from boarding flights,[164] or turned away at borders—often without ever being presented with evidence of any wrongdoing.[165] Moreover, are there accessible mechanisms to have the data effectively reviewed and, if appropriate, removed?

Former UN Special Rapporteur Fionnuala Ní Aoláin raised pointed concerns that the retention in a database of persons who travelled or attempted to travel to "jihadist conflict zones" did not seem to require that the respective person continue to pose a security risk, also at "the limited options that exist to have a person and their data removed from them." She specifically raised the potential adverse implications for people who have been registered in the database as children.[166]

Lawyers in the U.S. and Europe consulted for this research confirmed that getting people off No-Fly lists can be extremely difficult. Individuals put on such lists frequently face a legal black hole, they are denied access to the evidence against them and are left with little chance to challenge or rectify the situation and get remedy. In legal proceedings, intelligence agencies often shield behind an institutional culture of secrecy resistant to scrutiny and disclosure of information,[167] making due process nearly impossible.

Even where no conviction exists, the mere presence on a security list can lead to denied entry at foreign airports and unexplained deportations years later. One lawyer recounted the story of an adult client who, as an adolescent, had been persuaded by his family not to travel to Syria. Years later, now an adult, he was barred from entering a distant country for a holiday. There's no link whatsoever between his earlier attempted travel to Syria and the country where he was travelling to now. In similar cases, attempts to clear the names of clients with national intelligence services, INTERPOL, or the Schengen Information System proved challenging. As the lawyer put it: "When it becomes international, it's almost impossible to track down one's file abroad."[168] Also, the relatives of suspected persons who traveled to Syria are put on No-Fly lists.[169] In one case, a Swedish woman who had cooperated fully with authorities regarding her brother's travel to Syria was herself denied entry into Turkey while traveling on holidays with her children.[170]

The cost of such policies on family unity is illustrated by the case of J, an 18-year-old U.S. citizen. After traveling to Pakistan with his family, he was barred from returning to the U.S. and separated from his mother and siblings—because the FBI had ordered that he (and his father) be placed on the No Fly list based solely on a vague unverified allegation made by a relative during an interrogation. J had never been charged with a crime, let alone investigated.[171]

---

[164] Case of toddler stopped at airport at "Mistakes on Terrorist Watch List Affect Even Children" by Joe Sharkey, *New York Times*, Sept. 8, 2008 at https://heinonline.org/HOL/LandingPage?handle=hein.journals/huri34&div=35&id=&page=; *The Progress and Pitfalls of the Terrorist Watch List*, Field Hearing of the Committee on Homeland Security House of Representatives, one hundred tenth congress, first session, November 8 2007, at https://www.govinfo.gov/content/pkg/CHRG-110hhrg48979/html/CHRG-110hhrg48979.htm;

[165] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009.

[166] *Visit to Belgium, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/40/52/Add.5, 8 May 2019, para. 56.

[167] *Assessing Damage, Urging Action, Report of the Eminent Jurists Panel on Terrorism, Counter-terrorism and Human Rights, An initiative of the International Commission of Jurists*, Geneva 2009.

[168] Interview with lawyer.

[169] Interview with lawyer assisting returnees and families of persons who travelled to Syria.

[170] Interview with social worker.

[171] A cousin of his, who had been tried in the U.S. for alleged links with Jihadism, had suggested during an interrogation that J might have been part of a group of several Pakistani adolescents living in the U.S. whom he speculated had attended terrorist training camps in Pakistan. See "What's the Point of Being a Citizen?" in *Mrs. Shipley's Ghost, The Right to Travel and Terrorist Watchlists* by Jeffrey Kahn, The University of Michigan Press, 2013.

.

In fact, U.S. citizens placed on the No Fly List were found to "have suffered significantly[,] including long-term separation from spouses and children; the inability to access desired medical and prenatal care; the inability to pursue an education of their choosing; the inability to participate in important religious rites; loss of employment opportunities; loss of government entitlements; the in-ability to visit family; and the inability to attend important personal and family events, such as graduations, weddings, and funerals."[172] Further, according to the American Civil Liberties Union (ACLU), because the U.S. Terrorist Screening Dataset (TSDS) records are widely shared with law enforcement agencies throughout the U.S. and beyond, being on the No Fly List increases the risk of wider restrictions beyond traveling, including unlawful searches, surveillance, inability to open or maintain bank accounts, denial of government licenses or jobs, and indefinite delays or denials of immigration benefits, based on a questionable "reasonable suspicion".[173]

Stigmatization and reputational harm

What happens when a child is labeled a "security threat"? The answer can involve a lifetime of stigma and exclusion. In Iraq, for instance, the United Nations Development Programme (UNDP) has reported that the phrases 'ISIS families' or 'Daesh', which are widely used in official and popular Iraqi circles, "expose women and children to harassment, exclusion and marginalization and perhaps to attempts at retaliation now and in the future, just because they are or have been accused of being relatives of former ISIS members which is also in some cases a false accusation thrown for personal or tribal conflict reasons". In some cases, communities have required displaced mothers to abandon their male children as a condition for being allowed to return to their home area, even if the boy is only one day old.[174]

Being under surveillance is hugely stigmatising for a child.[175] A lawyer assisting children returning to Europe from Syria said, "data sharing is always dangerous because the person will be treated differently; the label always has an impact". Unlike juvenile offenses—which are typically sealed or forgotten with time—terrorism-related flags persist and follow individuals over time and even across borders.[176]

The emotional toll of these experiences cannot be underestimated. Lawyers and social workers have reported that their clients, often teenagers or young adults, feel deeply humiliated when turned away at airports in front of friends or family. So, the issue is not just protecting children´s privacy but also protecting them from stigma. Some have argued that the stigma and alienation associated to being labelled as an "extremist" or a "terrorist", or as affiliated with a terrorist or an extremist, in the long term may paradoxically have the opposite outcome sought, by increasing the risk of "radicalization" or violence rather than reducing it.[177]

Deprivation of other fundamental rights, including legal documentation, education and work

As mentioned, the consequences of watch listing can be wide-ranging. In Iraq, families perceived to be associated with ISIL have encountered administrative barriers that prevented them from obtaining security clearances to travel to their home areas and thus access legal documentation, including their IDs and children´s birth certificates. The children are consequently unable to enjoy their right to education and citizenship.[178]

---

[172] *Kashem*, 941 F.3d at 378 (citing one of the district court's prior decisions in the case, *Latif*, 28 F. Supp. 3d at 1149-50).

[173] *Brief for the American Civil Liberties Union and the ACLU Foundation of Oregon as Amicus Curiae supporting respondent in FBI v Yonas Fikre*. On immigration delays based on assessment of threat as a "national security concern", see *ACLU report on the Controlled Application Review and Resolution Program (CARRP)* at https://assets.aclu.org/live/uploads/2024/07/2024.07.10-CARRP-Delay-and-Deny15.pdf

[174] *Affiliated with ISIS: Challenges for the Return and Reintegration of Women and Children*, United Nations Development Programme Iraq, October 2022.

[175] Interview with expert on counterterrorism.

[176] Interview with lawyer.

[177] Interviews with lawyer and social worker dealing with child returnees from Syria.

[178] *Affiliated with ISIS: Challenges for the Return and Reintegration of Women and Children*, United Nations Development Programme Iraq, October 2022.

.

Former detainees at Guantanamo, including those who were underage at the time of their detention, have reported struggling with subtle forms of discrimination years after their release. Some have faced denial or great difficulties getting a passport, travelling to foreign countries, being unable to rent a home, or to get or keep a job.[179]

In Jordan, security services reportedly maintain a database that includes children and youth considered security threats and whose movements are monitored; it draws on intelligence from multiple partners.[180] It is reportedly not possible to know who is placed on the database, when, or why. Cases reported during this research illustrate the potential long term effect of such practices. A 17-year-old Syrian boy, arrested for a minor offense and held in a juvenile rehabilitation center in Jordan, later faced rejection from a public high school during his reintegration process. The school alleged security grounds but refused to provide any further explanation—even after a legal challenge. Today, at 23, he remains unemployed. Another case involved a Syrian man who applied for a position with an international NGO in Jordan, only to be denied a work permit on vague security grounds. Despite intensive legal action, the authorities refused to disclose the reason for the rejection.[181] According to his lawyer, a plausible explanation was the arrest of an extended family member in Syria—a tenuous association that may have led to his continued inclusion on a security list.

Discrimination

The discriminatory application of counterterrorism measures has come under increasing scrutiny. Former UN Special Rapporteur on human rights and counterterrorism indicated that "significant research has uncovered wide misuse and abuse of surveillance laws on a discriminatory basis, targeting particular communities and groups based on ethnic background, race and religion". She observed that such measures have not only targeted Muslim individuals but also spilled over to affect the rights of their families.[182]

The integration of Artificial Intelligence and algorithm-based statistics into transnational security frameworks may replicate and amplify existing biases and thus put children of a certain age-range, gender, country, race or religion at risk of discriminatory profiling, especially by border authorities.

This brings us to the issue of "discrimination by association." Introduced in EU jurisprudence through the *Coleman* case[183], the concept of discrimination by association refers to the situation of people who are at a disadvantage based on a proximity or association with someone else, over which they have no control. In that judicial case, a woman was found to have been discriminated against after she was dismissed from her job due to her child's disability, for whom she was the primary carer. The Court stated that although the person who is subject to direct discrimination on grounds of disability is not herself disabled, the fact remains that it is the disability which is the ground for the less favorable treatment which she claimed to have suffered.[184] Similarly, in various contexts,

[179] Interview with lawyer who assisted underage boys detained at Guantanamo prison; Interview with confidential source.

[180] Within the Global Counterterrorism Forum (GCTF), Jordan co-chairs the Foreign Terrorist Fighter Working Group together with the United States. See https://www.state.gov/reports/country-reports-on-terrorism-2022/jordan/

[181] Interview with INGO staff.

[182] *Human rights impact of counter-terrorism and countering (violent) extremism policies and practices on the rights of women, girls and the family, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin*. A/HRC/46/36, 22 January 2021, para. 11.

[183] *Coleman v. Attridge Law and Steve Law* (Case C-303/06).

[184] The judgment interprets the meaning of the prohibition of direct discrimination and harassment in employment and occupation on grounds of disability based on Article 2(2)(a) and Article 2(3) of Council Directive 2000/78/EC of 27 November 2000. See https://www.europeansources.info/record/the-concept-of-discrimination-by-association-and-its-application-in-the-eu-member-states/. See "Associative Discrimination in Britain and in the European Union: a still too Elastic Concept?" by Pierre de Gioia-Carabellese, Robert J. Colhoun in *E-Journal of International and Comparative Labour Studies*, Volume 1, No. 3-4 October-December 2012, pp. 248-261.

.

children of HIV-positive parents have faced discrimination, including denial of basic amenities, due to their association with the disease, even when the children themselves were not infected.[185]

Shouldn't the same reasoning on discrimination by association apply when children are watch listed or surveilled solely because their parent is a known or suspected terrorist?

Denial of asylum and international refugee protection

UN Security Council Resolution 1373 (2001) requires States to prevent the movement of terrorists through effective border controls (para. 2 (g)). It further requires that States take measures to ensure that refugee status is not granted to asylum seekers who have planned, facilitated or participated in terrorist acts (para. 3 (f) and (g)).[186]

International refugee law echoes this concern. Article 1(f) of the 1951 Refugee Convention provides for the exclusion of individuals who have committed grave crimes, including war crimes, serious non-political crimes, and acts contrary to the principles of the United Nations.[187] National authorities have relied on this prohibition to deny protection to individuals on grounds of their membership in a terrorist organization that committed war crimes, also sometimes relying on Security Council language that describes terrorism as inherently incompatible with UN principles.[188]

In this regard, former UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, emphasized that mere membership in a listed group or inclusion on a terrorist suspect list should not in itself or automatically trigger exclusion. An assessment of individual responsibility must be carried out on a case-by-case basis, with careful consideration of the role and personal involvement of the person concerned.[189]

Children are not exempt from refugee exclusion clauses, yet the application of such provisions must account for children´s unique vulnerabilities. According to UNHCR, exclusion can apply to children only if they have reached

---

[185] A study conducted by the Department of Rural Management in Jharkhand, India, showed that 35% of children of HIV-infected adults were denied basic amenities. See "AIDS Orphans and Vulnerable Children in India: Problems, Prospects, and Concerns" by Kumar, Anant in *Social Work in Public Health*, 2012; Case of the U.S. in "HIV-related stigma among people with HIV and their families: a qualitative analysis" by Laura M Bogart , Burton O Cowgill, David Kennedy, Gery Ryan, Debra A Murphy, Jacinta Elijah, Mark A Schuster, at https://pubmed.ncbi.nlm.nih.gov/17458691/; Case of Haiti in "Perceived discrimination and stigma toward children affected by HIV/AIDS and their HIV-positive caregivers in central Haiti" by Pamela J Surkan, Joia S Mukherjee, David R Williams, Eddy Eustache, Ermaze Louis, Thierry Jean-Paul, Wesler Lambert, Fiona C Scanlan, Catherine M Oswald, Mary Smith Fawzi, at https://pubmed.ncbi.nlm.nih.gov/20635244/

[186] Convention Relating to the Status of Refugees and its 1967 Protocol. See https://www.unodc.org/e4j/en/terrorism/module-3/key-issues/international-refugee-law.html

[187] Article 1 (f) of the 1951 Refugee Convention (known as the exclusion clauses) states that "the provisions of this Convention shall not apply to any person with respect to whom there are serious reasons for considering that:
(a) he has committed a crime against peace, a war crime, or a crime against humanity, as defined in the international instruments drawn up to make provision in respect of such crimes;
(b) he has committed a serious non-political crime outside the country of refuge prior to his admission to that country as a refugee;
(c) he has been guilty of acts contrary to the purposes and principles of the United Nations".

[188] Security Council resolution 1373 states that "acts, methods and practices of terrorism are contrary to the purposes and principles of the United Nations" and that "knowingly financing, planning and inciting terrorist acts are also contrary to the purposes and principles of the United Nations".

[189] *Report of the Special Rapporteur of the Human Rights Council on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson*, A/71/384, 13 September 2016, para. 27.

.

the age of criminal responsibility and are mentally capable of understanding their actions. Exclusion decisions regarding children should also include careful consideration of defenses such as duress.[190]

There are examples where childhood membership in a terrorist-designated armed group that engaged in war crimes has led to exclusion. In the UK, for instance, a Sri Lankan man who had been recruited at the age of ten into an armed group was denied asylum. The Supreme Court held that determining factors were, *inter alia*, how the asylum-seeker came to be recruited, the length of time he remained in that organization and what, if any, opportunities he had to leave it, his position, rank, standing and influence in the organization, his knowledge of the organization's war crimes activities, and his own personal involvement and role in the organization including particularly whatever contribution he made towards the commission of war crimes.[191]

In Canada, an Iranian citizen who, as an adolescent, had been a "member of an organization that there were reasonable grounds to believe engages, has engaged or will engage in acts of terrorism", was found inadmissible under national immigration law. As a boy, the appellant had been allowed by the group to distribute propaganda leaflets once or twice a month until he was almost 18 but stopped after he was arrested and detained by the police. The Court said that the term "member" was to be given a broad and unrestricted interpretation given that, in immigration legislation, public safety and national security are highly important. It further stated there was a presumption that the closer the child is to 18 years of age, the greater the likelihood that the child will possess the requisite knowledge or mental capacity.[192]

A concern with invoking terrorism grounds in asylum decisions is the broad and often vague definition of terrorism in national laws. Additionally, with the interoperability of law enforcement, immigration, and asylum information systems, placing children formerly recruited by terrorist groups in security databases could jeopardize their future asylum claims.

VI. Regulatory frameworks

This section invites reflection on whether existing regulatory frameworks adequately protect children´s rights when counterterrorism measures involve the collection, storage, or use of children´s personal data.

A key finding of this research is the gap in how current data protection frameworks in national security and counterterrorism contexts address children's rights. While international standards provide strong protections for children in judicial settings, there are no clear, binding international rules governing administrative measures[193] towards children—such as watch listing or travel bans—which can significantly affect children with past, presumed,

---

[190] *UNHCR Guidelines on International Protection: Application of the Exclusion Clauses: Article 1F of the 1951 Convention relating to the Status of Refugees*, September 2003. According to the UNHCR Guidelines, "the fact that an individual is designated on a national or international list of terrorist suspects (or associated with a designated terrorist organisation) should trigger consideration of the exclusion clauses but will not in itself generally constitute sufficient evidence to justify exclusion. Exclusion should not be based on membership of a particular organisation alone, although a presumption of individual responsibility may arise where the organisation is commonly known as notoriously violent and membership is voluntary. In such cases, it is necessary to examine the individual's role and position in the organisation, his or her own activities…" (para. 26).

[191] https://www.supremecourt.uk/cases/docs/uksc-2009-0121-press-summary.pdf
https://ukscblog.com/case-comment-r-jssri-lanka-v-secretary-of-state-for-the-home-department/

[192] *Poshteh v. Canada* (Minister of Citizenship and Immigration) (F.C.A), 2005 FCA 85.

[193] The term "administrative measures" often refers to coercive measures that may restrict the exercise of certain human rights, irrespective of the laying of criminal charges, against a person perceived to pose a risk to national security, such as travel bans like preventing travel abroad, preventing an individual's return to their State, deprivation of nationality, administrative detention, and airport stop-and-search powers. See *Terrorism and human rights, Report of the United Nations High Commissioner for Human Rights*, 7 August 2024.

.

or familial links to armed groups designated as terrorist. For example, while there is a well-established rule requiring States to set a minimum age of criminal responsibility, there is no similar rule to establish a minimum age for collecting children's personal data for counterterrorism purposes.

General data protection laws often acknowledge that children need heightened protection as children. However, when it comes to counterterrorism regulatory frameworks, specific safeguards for children's data are rarely detailed.[194] It could be argued that it's not possible not to have similar detailed safeguards for children in such frameworks, where the risks are equal or even higher.

While national security exemptions in data protection laws permit States to override most data protection rights, these exemptions are not a *carte blanche*: even in such cases, data controllers and processors remain accountable under core data protection principles, national security and law enforcement legislation, and, crucially, international human rights law, especially where international treaties carry superior legal authority in domestic legislation.

International human rights standards protect children's rights related to personal data, including in counterterrorism contexts, as outlined below. Annex II highlights key provisions from relevant EU and other regulatory frameworks. Together, these offer a basis for critically assessing current protections and identifying gaps that need to be addressed.

Children´s rights and personal data protection under International Human Rights Law

Child rights´ guiding principles

A fundamental principle of international law is the best interests of the child, enshrined in Article 3 of the nearly universally ratified[195] UN Convention on the Rights of the Child (CRC), which requires that children's best interests be a primary consideration in all judicial, administrative, and legislative actions concerning the child.[196] This applies to all governmental decisions affecting children, including about the collection and use of their personal data. The obligation remains binding even in armed conflict and counterterrorism contexts.[197]

Under the principle of non-discrimination, children must be protected from all forms of discrimination or punishment including based on the status, activities, expressed opinions, or beliefs of the child's parents, legal guardians, or family members (Article 2.2 of the CRC). Hence, children cannot be discriminated against because of their familial ties to known or suspected terrorists.[198]

Article 12 of the CRC affirms children's right to be heard in all matters affecting them. However, if national security exemptions prevent children from accessing or challenging the data held about them, this may directly undermine both their right to be heard (Article 12) and their right to seek and receive information (Article 17).

Children's right to privacy

[194] Interview with Thomas Wahl from Max Blanck Institute.

[195] Except for the United States.

[196] Convention on the Rights of the Child, Art.3.1 : "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."

[197] *Children and Counter terrorism*, UNICRI, 2016, p.16.

[198] *Handbook, Children affected by the foreign-fighter phenomenon: Ensuring a child rights-based approach*, United Nations Office on Counterterrorism, UN Counterterrorism Center.

.

International human rights law permits lawful limitations on the right to privacy,[199] and it is, moreover, a derogable right during states of emergency.[200] The UN Human Rights Committee (CCPR), which monitors implementation of the International Covenant on Civil and Political Rights (ICCPR), has affirmed that the right to privacy under Article 17 is not absolute, yet any interference must meet strict conditions. Similarly, the European Court of Human Rights (ECHR), interpreting Article 8 of the European Convention on Human Rights, has developed detailed criteria for permissible limitations.

Both bodies require that any interference must be provided for by law – the law must be accessible, clear, and non-arbitrary; it must serve a legitimate purpose, such as protecting national security, or the rights of others; it must be necessary in a democratic society and proportionate – meaning it must respond to a pressing social need, and be reasonable in the particular circumstances.[201]

Hence, as emphasized by the former UN Special Rapporteur on counterterrorism and human rights, invoking terrorism does not grant a *carte blanche* for surveillance. Each interference must meet strict tests of legality, necessity, and proportionality.[202] While proportionality allows for a margin of appreciation, in balancing a legitimate end like national security against the individual´s right to privacy key red lines remain: Are less intrusive means available to achieve the legitimate aim? Are there safeguards, like independent judicial oversight and access to redress? Is the interference not indiscriminate, and non-discriminatory?[203]

The European Charter of Fundamental Rights goes further, establishing the right to data protection as a distinct stand-alone right. And certain States, such as Argentina and Portugal, even recognize data protection as a constitutional guarantee.[204]

This right to data protection, in addition to requiring that data collection is lawful, fair, for a legitimate aim and necessary, it requires transparency of data processing procedures; to limit the use of data to the purpose for which data was recorded; to minimize the amount of data collected or recorded; accuracy and updating of data; that data be retained for no longer than is necessary to fulfil the purpose for which it was recorded;[205] accountability; and security of the data, meaning integrity and confidentiality.[206]

Specifically with regard to children, the UN Convention on the Rights of the Child (CRC) makes clear that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence,

---

[199] Article 17 of the ICCPR; Article 8 of the European Convention on Human Rights; Article 52 of the EU Charter on Fundamental Rights.

[200] For example, France has invoked the state of emergency declared after terrorist attacks to place individuals on the "fiche S" list (with "S" standing for *Sûreté de l'État*, or State security), allowing for the surveillance of those considered national security threats. Interview with Basile de Bure.

[201] UN Human Rights Committee: General Comment No. 16 (1988) on Article 17; CCPR/C/USA/CO/4; CCPR/C/FRA/CO/5; *I.R. and Others v. Republic of Korea* (CCPR/C/130/D/2625-2626/2015); *van Hulst v. Netherlands* (CCPR/C/110/D/2179/2012). EUCHR: *Klass and Others v. Germany* (1978); *Szabó and Vissy v. Hungary* (2016); *Malone v. the United Kingdom* (1984); *S. and Marper v. the United Kingdom* (2008); *Roman Zakharov v. Russia* (2015); *Big Brother Watch and Others v. the United Kingdom* (2021); See *Guide on Article 8 of the European Convention on Human Rights*, 31 August 2024; *Guide to the Case-Law of the of the European Court of Human Rights - Data protection*, 31 August 2024.

[202] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/13/37, 28 December 2009, para. 13.

[203] See for instance CCPR Concluding Observations on the USA (2014), CCPR/C/USA/CO/4, para. 22; CCPR/C/FRA/CO/5, para. 12; *Digital Rights Ireland Ltd v. Ireland*, CJEU Case C-293/12 (2014); EUCHR: *Vavřička and Others v. the Czech Republic* [GC], 2021.

[204] Article 43 of the Argentinean Constitution and article 35 of the 1976 Constitution of Portugal.

[205] *Guide to the Case-Law of the European Court of Human Rights - Data protection*, 31 August 2024.

[206] EU General Data Protection Regulation (GDPR) and Council of Europe Convention 108+. *The Keys to Data Protection*, *A Guide for Policy Engagement on Data Protection*, Privacy International, August 2018.

.

nor to unlawful attacks on his or her honor and reputation. The child has the right to the protection of the law against such interference or attacks" (CRC Art.16). In this light, the UN Committee on the Rights of the Child has clarified that any interference with a child´s privacy must be lawful, proportionate, and in the best interests of the child, and must not conflict with the provisions, aims or objectives of the Convention.[207] The Committee further stated that children's data gathered for defined purposes, in any setting, including digitized criminal records, should be protected and exclusive to those purposes and should not be retained unlawfully or unnecessarily or used for other purposes.[208]

These protections of the right to privacy should apply with even greater force in counterterrorism contexts, where the risks of harm and stigmatization are especially high.

Children´s right to be protected from unlawful recruitment and exploitation by armed groups

This research particularly focuses on data from children allegedly associated with armed groups. Children associated with any armed groups are, first and foremost, victims under international law—regardless of whether those groups are designated as terrorist. Those recruited and exploited by terrorist-designated groups should be further recognized as victims of terrorism.[209] International human rights law and international humanitarian law prohibit, and customary international criminal law (ICL) criminalizes—the recruitment of children under 15 by armed forces or groups, as well as their use in hostilities.[210] The Optional Protocol to the CRC on the Involvement of Children in Armed Conflict (ratified by 172 States),[211] prohibits all recruitment —forced or voluntary— of children under 18 by non-state armed groups, and obliges States to support their recovery and reintegration.[212]

Aligned with this legal framework, the Paris Principles and Guidelines on Children Associated with Armed Forces or Armed Groups (known as the "Paris Principles") —endorsed by over 100 States[213]—affirm that "children who have been associated with armed forces or armed groups should not be prosecuted or punished or threatened with prosecution or punishment solely for their membership in those forces or groups". If they have committed serious crimes while associated with armed groups, they must be treated in line with international child justice standards.[214]

The UN Committee on the Rights of the Child has similarly urged States not to prosecute children for mere association with non-state armed groups, including those designated as terrorist, or for expressions of opinion.[215]

---

[207] Committee on the Rights of the Child, General comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021.

[208] *Ibid,* para. 73.

[209] *Strengthening Human Rights in Counter-Terrorism Strategy and Policy: A Toolkit*, United Nations Office of the High Commissioner for Human Rights.

[210] The recruitment and use of children in hostilities is prohibited by the Convention on the Rights of the Child (Art. 38), the African Charter on the Rights and Welfare of the Child (Art. 22.2) and the Optional Protocol to the CRC on Children and Armed Conflict (Art.4). Forced conscription of children under 18 is prohibited under the ILO Worst Forms of Child Labor Convention No. 182 of 1999 (Art. 3. a). Under IHL, Additional Protocol I to the Geneva Conventions (Article 77(2)) in international armed conflict, Additional Protocol II to the Geneva Conventions (Article 4(3) (c)) in internal armed conflict and Rule 136 of Customary IHL prohibit the recruitment of children under 15. Under the Statute of the International Criminal Court, conscripting or enlisting children under 15 into armed forces or groups constitutes a war crime in both international and non-international armed conflicts (article 8, para. 2, *(b)* (xxvi) and *(e)* (vii)).

[211] https://indicators.ohchr.org/.

[212] Article 6.3 of the Optional Protocol to the CRC on the Involvement of Children in Armed Conflict (OPAC).

[213] The Paris Principles and Guidelines on Children Associated with Armed Forces or Armed Groups, February 2007. https://childrenandarmedconflict.un.org/publications/ParisPrinciples_EN.pdf

[214] Para. 8.7 of the Paris Principles; Resolution adopted by the General Assembly on 22 June 2023, The United Nations Global Counter-Terrorism Strategy: eighth review A/RES/77/298, para. 121.

[215] Committee on the Rights of the Child, General comment No. 24 (2019) on children's rights in the child justice system, CRC/C/GC/24, 18 September 2019, paras. 97-101.

.

Likewise, the UN Secretary-General has been unequivocal: "children should not be detained or prosecuted solely for their association with or membership in any armed group, including designated groups", stressing that children's best interests require prioritizing rehabilitation and reintegration.[216] This position is echoed by both the UN Human Rights Council[217] and the UN Security Council.[218] Notably, Security Council Resolution 2331 affirms that victims of trafficking by terrorist groups should be recognized as victims of terrorism and not penalized or stigmatized for unlawful acts they were compelled to commit.[219]

The above standards do not preclude justice measures for children who are above the minimum age of criminal responsibility alleged to have committed serious crimes while associated with armed groups.

Child rights in the justice system

In child justice systems, a child below the minimum age of criminal responsibility cannot be prosecuted.[220] This protection seems not to systematically extend to children´s data collection for counterterrorism purposes. When it comes to personal data collection and processing on national security grounds, including placement in watch lists, there is no shared stand to have a minimum age.

International child justice standards also emphasize confidentiality.[221] Children´s identifying information should be redacted from public documents, files, and court dockets.[222] Once sanctions or measures end, case records should be destroyed or archived with restricted access, limited to the child, their guardians, and authorized officials. Prosecutors should not rely on information contained in these records to pursue charges once the child becomes an adult.[223] The UN Committee on the Rights of the Child has further recommended that States refrain from listing details of any child—or anyone who was a child at the time of the offense—in public offender registers or other public registers that hinder opportunities for reintegration.[224]

The core principle underlying these protections is that safeguarding a young offender's privacy is essential for rehabilitation. This, along with the rights to be presumed innocent and treated with dignity[225]—cornerstones of child justice—is compromised when children are placed on watch lists based on a perceived potential risk, such as due to family ties to terrorist groups.

The right to be forgotten

---

[216] *Key Principles for the Protection, Repatriation, Prosecution, Rehabilitation and Reintegration of Women and Children with links to United Nations Listed Terrorist Groups*, UN Secretary General, April 2019.

[217] Resolution 49/20 "Rights of the child: realizing the rights of the child and family reunification" adopted by the Human Rights Council on 1 April 2022.

[218] Security Council Resolution 2427 (2018), para.20.

[219] Security Council Resolution 2331 (2016) on trafficking in persons in conflict situations, para.2 (d).

[220] The CRC in Article 40(3)(a) provides that States Parties shall establish a minimum age below which children shall be presumed not to have the capacity to infringe the criminal law.

[221] Rule 21 of the United Nations Standard Minimum Rules for the Administration of Juvenile Justice (Beijing Rules) specifically emphasizes the "duty under international child justice standards to make sure information and records of young offenders are kept strictly confidential and closed to third parties".

[222] *IIJ Juvenile Justice Practitioner's Notes: Prosecutors,* The International Institute for Justice and the Rule of Law.

[223] CRC Committee General comment No. 24 (2019) on children's rights in the child justice system, paras. 67 and 71; Council of Europe's Recommendation CM/Rec (2008) 11 of the Committee of Ministers to Member States on the European Rules for juvenile offenders subject to sanctions or measures, at 34.2.d.

[224] CRC Committee General comment No. 24 on children's rights in the child justice system, 18 September 2019, para. 69.

[225] In CRC Article 40, States recognize "the right of every child alleged as, accused of, or recognized as having infringed the penal law to be treated in a manner consistent with the promotion of the child's sense of dignity and worth", as well as "the right of every child to be presumed innocent until proven guilty according to law".

.

In some cases, regional and national legal frameworks have advanced beyond international standards, offering stronger protections, such as establishing the "right to be forgotten". The right to be forgotten refers to the right to have publicly available data deleted. In the European Union, for instance, an early version of the right to be forgotten evolved into the more limited "right of erasure" under Article 17 of the General Data Protection Regulation (GDPR). This provision allows individuals to request the deletion of personal data under specific conditions and explicitly applies when the data was shared by the individual while he or she was a child.[226]

This concept gained further traction through legal precedent. In the *Costeja v. Google* case (2014), the European Court of Justice recognized the right to be forgotten as a human right.[227] Beyond the EU, the state of California in the U.S. has legalized the right to be forgotten specifically for children,[228] and a similar initiative was proposed in the UK in 2017.[229] The idea behind the right to be forgotten, in the context of social media, is the acknowledgment that children sometimes make immature decisions and should not be forever trapped or defined by them.[230]

Although the use of children's data for security purposes often escapes public attention, the consequences can be just as harmful as public exposure. Such use of data can seriously hinder a child's chances of reintegration, education, and future employment. By analogy, children unlawfully recruited or used by armed groups, as well as children of convicted or presumed "terrorist" parents, may have a legitimate claim to a right to be forgotten—that is, to the erasure of data that compromises their privacy and puts them at risk of discrimination. Shouldn't they too be given the chance to move on, especially beyond a past they may have not chosen? The right to be forgotten could be a vital step toward reintegration.

VII. Options

Rethinking the use of children's personal data in counterterrorism — a Rights-Based reset

This research finds that children's personal data has been collected for counterterrorism purposes in various conflict and post-conflict settings. These practices can cause lasting harm, undermining children's rights to privacy and other fundamental freedoms, while also reinforcing stigma.

Current counterterrorism frameworks often include broad, non-specific provisions—such as the requirement to consider the best interests of the child when dealing with children´s personal data, or that specific safeguards should be adopted for vulnerable persons, including children. But are these general provisions sufficient? Is there a need for clearer, binding rules—rooted in children's rights—that provide concrete guidance to those handling children´s data and making the required best interest determinations?

This section explores practical options as possible ways to strengthen child rights protections in the use of personal data for counterterrorism purposes.

Should there be a minimum age for security-based personal data collection?

One proposal worth considering is setting a minimum age below which children's personal data cannot be collected for counterterrorism purposes. If the law recognizes that children under a certain age cannot be held

[226] Article 17 of the GDPR, Recital 65.
[227] See https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf
[228] California's Online Eraser Law of 1 January 2015. This Law allows children in California who are registered users to request removal of content or information they posted on an operator's website, application, or online service. https://www.lexology.com/library/detail.aspx?g=5c1e37a5-3b96-4b52-84df-5b5c89a4f2f7.
[229] In 2017, former UK Prime Minister Theresa May campaigned to expand privacy rights for children to allow them to delete information, arguing that social media sites store data that can affect children´s lives over time, such as at job applications. https://www.theguardian.com/media/2015/jul/28/ministers-back-campaign-under-18s-right-delete-social-media-posts
[230] Discussion with Professor Jonathan Todres.

.

criminally responsible, it seems inconsistent—and arguably unjust—to retain their data in secret profiles, watch lists, or databases based on speculative risks or family ties (with the associated control and potential restriction of rights). Even when a child has committed an offence, child justice systems are founded on a belief that children can be rehabilitated. To support this, children must be given genuine opportunities to reintegrate into society, not placed under indefinite suspicion or stigmatizing surveillance.

However, using the minimum age of criminal responsibility (MACR) as the default threshold presents certain challenges. MACRs highly vary across jurisdictions: set, for instance, at 7 in Nigeria and Yemen,[231] 10 in Syria,[232] and 11 in the Kurdistan Region of Iraq.[233] In Europe, the MACR spans from 10 (in England),[234] 12 (in Belgium, the Netherlands, and in Hungary in relation to specific criminal offences, including certain acts of terrorism)[235] to 14 (in countries like Austria and Germany).[236] This lack of harmonization creates a protection gap: it would leave many children unprotected in countries that set MACR at a low age. And still, where laws regulating intelligence services include specific rules on children, as in Germany, they may set different minimum ages for activities like transmitting, storing, or retaining children's data.[237]

Could an international baseline help? It could be agreed that no child under 18—the widely recognized age of majority—should be subject to counterterrorism-related data collection, particularly when this is based solely on presumed threats arising from past recruitment or family connections to a terrorist group. However, some would argue that a blanket ban goes too far, as some children could pose a genuine risk. In those specific cases, a case-by-case assessment might offer a more balanced approach. Such assessments would require substantial investment in resources and expertise within security and counterterrorism bodies—similar to the individualized evaluations used in refugee and migration systems for child asylum seekers. Ultimately, adopting a psychosocial or public health approach for these children may be more effective and humane than one driven primarily by law enforcement.

Setting a minimum age at least at 14 or 16, as recommended by the UN Committee on the Rights of the Child for criminal responsibility,[238] might offer a pragmatic starting point. And where age is uncertain the child should receive the benefit of the doubt.

Should children's data be categorized as "sensitive" data?

Another potential safeguard is to formally classify children's personal data as "sensitive data" under data protection laws. Sensitive data – such as information revealing the person´s race or ethnicity, political opinions,

---

[231] Yemen Republican Decree, Law No. 12 of 1994 concerning crimes and penalties, Section 31; Section 30 of the Nigerian Criminal Code.

[232] Juvenile Act 1974, Article 10 (as amended by Legislative Decree No. 52 of 2003).

[233] Article 47(1) of the Juvenile Welfare Law No. 76 of 1983

[234] *Systematic Responses to Children under the Minimum Age of Criminal Responsibility who have been (Allegedly) Involved in Offending Behaviour in Europe and Central Asia*, UNICEF Regional Office for Europe and Central Asia.

[235] *Minimum Ages of Criminal Responsibility in Europe* at https://archive.crin.org/en/home/ages/europe.html

[236] https://archive.crin.org/en/home/ages/europe.html

[237] For instance, according to German legislation regulating intelligence services, data on children under 14 may be transmitted only in specific exceptional circumstances; data on the behavior of children under the age of 14 may not be stored in files, and data on children below 16 stored in files must be deleted after two years. See https://www.gesetze-im-internet.de/bverfschg/__11.html; https://www.gesetze-im-internet.de/bverfschg/__24.html; https://www.gesetze-im-internet.de/bndg/__65j.html

[238] CRC Committee General comment No. 24 (2019) on children's rights in the child justice system. The UN Committee on the Rights of the Child has encouraged States parties to take note of recent scientific findings, and to increase their minimum age accordingly, to at least 14 years of age, regardless of the gravity of the offence. And if there is no proof of age and it cannot be established that the child is below or above the minimum age of criminal responsibility, to give the child the benefit of the doubt and not be held criminally responsible. It further states that "the developmental and neuroscience evidence indicates that adolescent brains continue to mature even beyond the teenage years, affecting certain kinds of decision-making. Therefore, the Committee commends States parties that have a higher minimum age, for instance 15 or 16 years of age, and urges States parties not to reduce the minimum age of criminal responsibility under any circumstances, in accordance with article 41 of the Convention" (para. 22).

.

trade-union membership, religious or other beliefs, health, sexual life, criminal history, and biometric data[239] – triggers heightened protections, due to the significant risks its use could pose to the individual´s fundamental rights and freedoms.[240]

Given the serious impact on children´s rights of using children's data for counterterrorism purposes, such data could meet the threshold of sensitivity. Data on children formerly associated with armed groups could even qualify under sensitive data revealing "political opinions", especially where courts have recognized that mere past association with a group may suffice.

Recognizing children's data as sensitive would require strict limits on its use, subject to strict purpose limitation set by law, with only exceptional cases allowing processing, and a limited data retention span (after a short or predefined period of time the data would be deleted or anonymized). It would also trigger stronger special safeguards such as professional secrecy, risk assessments, and robust encryption standards.

Is there ever a justifiable reason to place a child on a watchlist?
Can placing children on security watchlists ever serve their best interests? The evidence suggests not. As shown, watch listing often results in stigma, surveillance, and rights´ restrictions, with no clear gains in public safety. Zero risk is unattainable, even if all children with links to armed groups were listed. Instead, States could invest more in reintegration support as a form of prevention.

It seems hence more consistent with upholding the children´s best interests excluding all children under 18 from watch lists. And where necessary, in exceptional cases, inclusion in such lists may be permitted following rigorous, case-by-case assessment and regular review. This measure would need to be subject to independent oversight by a public authority mandated to protect children's rights—such as an ombudsperson—or ensure children´s rights experts are included within the oversight body, as recommended by former Special Rapporteur Fionnuala Ní Aoláin.[241]

Enforcing strict rules on confidentiality and protection of children´s data
If a child is convicted of an offence, child justice standards require strict confidentiality of their personal data. This would mean such data should not be shared for watch listing or other counterterrorism purposes. Where State agencies must share information for coordination of rehabilitation or reintegration interventions, they must all adhere to the same stringent confidentiality and data protection standards.[242]

It also makes sense that heightened protections for children´s data should apply just as much to third-party contractors—often the ones collecting biometric data on behalf of governments.[243] The U.S. military for instance, has relied heavily on private contractors to carry out biometric data collection in Afghanistan and Iraq.[244] These private actors should not operate in a regulatory vacuum regarding children´s data.

---

[239] The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), Art. 6. https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[240] Art. 9 of the GDPR. Such protections include Data Protection Impact Assessments (DPIAs), required when processing is likely to result in a high risk to individuals' rights and freedoms; Enhanced security measures, including encryption, pseudonymization, and strict access controls; Transparency and accountability, requiring clear documentation of processing activities and purposes. See https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/
[241] "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" by Krisztina Huszti-Orban and Fionnuala Ní Aoláin, Human Rights Center, University of Minnesota, 2020, p. 22.
[242]Council of Europe Recommendation of the Committee of Ministers to Member States concerning new ways of dealing with juvenile delinquency and the role of juvenile justice, 24 September 2003, Article 21.
[243] *Safeguards for Public-Private Surveillance Partnerships*, Privacy International, December 2021.
[244] *Biometrics and Counter-Terrorism Case study of Iraq and Afghanistan* by Privacy International, May 2021.

.

Explicit protection of children´s data in "handover protocols"

Handover protocols signed between the UN and national governments in various countries require the rapid transfer of children allegedly associated with armed groups, by security forces to child protection actors. The protocols permit security forces to collect only minimal identification data when they encounter children. However, these agreements are not legally binding; also security forces are typically the first to encounter and engage with children exiting armed groups without the presence or oversight of child protection personnel.[245] As a result, broader collection of children´s data for security purposes is likely. Key questions arise: For how long and for what purpose is the data collected? Who has access to the information gathered by security forces? How secure is the data? Including strong data protection provisions in handover protocols, including limits to data retention, use and sharing, could help ensure that such data is subject to strict safeguards—based on legality, purpose limitation, necessity, and proportionality. This could also help prevent children from being placed on security databases or watch lists, and having their data eventually transferred across borders.

Are security actors well equipped to handle children's data?

Security and counterterrorism agencies may simply lack the tools or the capacity to apply child rights principles in data practices. The UN Security Council's Counterterrorism Executive Directorate (CTED), who conducts regular assessments of States´ implementation of counterterrorism resolutions, could evaluate how States handle children's personal data. In its engagement with States, CTED could also facilitate access to technical assistance on children´s data protection.

UN bodies providing capacity building on counterterrorism issues, as well as NATO, could integrate child rights training by child protection experts, including on age verification and data protection, in their programs. Such training should emphasize that children recruited by armed groups are primarily victims and must be treated as such, regardless of the group's designation as terrorist.

National, regional and international agencies involved in collecting or processing personal data for security purposes could invest in staff training on child rights´ standards, including the presumption of innocence and confidentiality of children´s data on criminal records, irrespective of the gravity of the offence.

Exploring the gender dimensions of data collection

The gender dimensions of children's data collection in conflict deserve greater scrutiny. Adolescent boys seem particularly at risk of having their personal data collected and used for counterterrorism purposes. This is largely because boys make up most of the children detained on national security grounds, and they are often classified as "military-age males." Girls, on the other hand, may be penalized for their association with fighters through forced or coerced marriages. In Iraq, for example, counterterrorism laws have been used to criminalize girls and women accused of "harboring" terrorists—sometimes simply for carrying out domestic tasks for their spouses who are members of terrorist groups.[246]

Broader child protection measures affecting data use

Other broader measures protecting children´s rights in armed conflict and counter terrorism contexts could positively impact on the protection of children´s data.

---

[245] Interviews with former UN workers in the Lake Chad Basin and the Sahel.

[246] Iraqi Counter-Terrorism Act No. 13 (2005), Article 4.2: "Anyone, who intentionally covers up any terrorist act or harbors a terrorist with the purpose of concealment, shall be sentenced to life imprisonment"; *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, submitted in accordance with Assembly resolution 72/180 and Human Rights Council resolution 49/10*. A/77/345, 16 September 2022.

.

If children recruited by terrorist-designated armed groups are legally recognized as victims and, if prosecuted at all, they are handled within civilian child justice systems—regardless of the offence's severity—the justification for collecting, storing, or sharing their personal data for counterterrorism purposes would become weaker. This highlights the need to criminalize the recruitment of anyone under 18 by armed groups in domestic law, and to explicitly exclude children from the scope of antiterrorism laws and from exceptional antiterrorism jurisdictions.[247]

Finally, perhaps the conversation on security needs reframing: not around whether children could pose a threat, but whether security systems can pose a threat to children, casting shadows that may persist long after conflict ends.

[247] UN Human Rights experts have advocated that States should explicitly exclude children from national counter-terrorism and security legislation and ensure that children who are above the minimum age of criminal responsibility and may have committed terrorism-related offences are treated exclusively within child justice systems, rather than within military, intelligence or national security courts. See *Strengthening Human Rights in Counter-Terrorism Strategy and Policy: A Toolkit*, United Nations Office of the High Commissioner for Human Rights, p.15.

.

Annex I – Country examples

Iraq

As of January 2021, around 2,294 children were detained by the Federal Government of Iraq for alleged involvement with ISIL.[248] And by the end of 2023, at least 668 children (663 boys, 5 girls) were verified as remaining in detention on national security charges, including for their alleged association with armed groups, primarily ISIL. Most were boys aged 15 to 17, though some were as young as 9.[249]

Iraqi children have also been detained in Syria due to alleged association with ISIL or family ties with the armed group. In March 2023, Iraq repatriated at least 203 boys from northeast Syria via prison transfers, and some were prosecuted under Iraqi anti-terrorism laws upon return.[250] Many others still remain in Syrian camps due to their parents´ alleged links to ISIL, in conditions possibly amounting to cruel or inhuman treatment.[251] Though not charged with crimes, these children are often seen as "security risks" with suspicion, anger, and fear from their communities.[252]

Iraqi anti-terrorism legislation includes broad, vague definitions of terrorism and does not distinguish between adults and children. Article 4 of the 2005 Iraqi Anti-Terrorism Act and Article 3(7) of the Kurdistan Region's law have led to broad and arbitrary interpretations of membership and led to children being arrested on suspicion of loose links to ISIL.[253] Children have been thus prosecuted under anti-terrorism legislation for actions such as taking an oath imposed by ISIL or, in the case of girls, for receiving salaries paid by ISIL to the wives of its members—actions interpreted as support for the group.[254] Sole membership can lead to up to 5 years of imprisonment and participation in armed action while associated to a terrorist group can lead to a sentence of 5 to 15 years' imprisonment.[255]

Iraqi authorities maintain security databases containing personal data of individuals suspected of ISIL links, including children. In 2018, Arab boys from communities that security forces associate with ISIL were routinely

[248] *Bridging the Gap: Bringing the Response to Children Formerly Associated with ISIL in Iraq in Line with International Child Protection Standards*, Watchlist Policy Note 2021.
[249] *Secretary-General Annual Report on Children and Armed Conflict 2024*.
[250] *Secretary-General Annual Report on Children and Armed Conflict 2024*.
[251] Reports of the Independent International Commission of Inquiry on the Syrian Arab Republic: A/HRC/54/58, para 98; A/HRC/52/69 para. 121; A/HRC/55/64 para. 110.
[252] "Distinguishing Children From ISIS-Affiliated Families in Iraq and Their Unique Barriers for Rehabilitation and Reintegration" by Joana Cook in *Perspectives on Terrorism* Volume XVII, Issue 3, September 2023.
[253] Under Article 4 of the Iraq Federal Anti-Terrorism Law, children are sometimes charged with mere association with ISIL, without regard to whether they committed a violent crime. See *Bridging the Gap: Bringing the Response to Children Formerly Associated with ISIL in Iraq in Line with International Child Protection Standards*, Watchlist Policy Note 2021. In each case of 23 individuals released under the Iraqi amnesty law, the defendants had confessed to participating in ISIL training for between 7 and 30 days before turning 18, but there was no evidence that they engaged in other ISIL activities. In case 118\GH.M\2020, the defendant admitted that he had participated in a one-month training with ISIL in 2014, when he was under the age of 15. The committee judges found that "the accused minor was not yet 15 years old at the time and didn't comprehend the results of his actions, and that merely taking a course without carrying out any terrorist activity cannot be considered affiliation." *Human Rights in the Administration of Justice in Iraq: Trials under the anti-terrorism laws and implications for justice, accountability and social cohesion in the aftermath of ISIL*, United Nations Assistance Mission for Iraq Office of the United Nations High Commissioner for Human Rights, January 2020, Baghdad, Iraq
[254] Interview conducted by the author in 2021 with a local organization working on child justice in northern Iraq.
[255] The UN reported the case of a juvenile who was condemned to 15 years of imprisonment after admitting that his father, mother and three brothers were part of a group of civilians that "supported ISIL' by acting as human shields to protect a group of ISIL fighters from airstrikes. Trial observed on 23 May 2019 in Karkh Juveniles court in Baghdad. See *Human Rights in the Administration of Justice in Iraq: Trials under the antiterrorism laws and implications for justice, accountability and social cohesion in the aftermath of ISIL*, UNAMI/OHCHR, January 2020.

.

stopped at checkpoints and checked against extensive “wanted lists” compiled by various security agencies. “Names could be included on these lists for involvement with ISIL in any capacity, including as a driver, cook or other non-combatant role, or if a relative – however distant – was involved with ISIL.”[256] Amnesty International reported that boys were arrested at screening sites in cases of mistaken identity, i.e., if their name was the same or similar to the name of a suspect on the ’wanted list’; some of the boys were then detained, tortured, or summarily executed.[257] Some who served prison terms as children remained on wanted lists after release, this restricting their movement. For instance, four individuals who had been arrested as children and had served three to five-year prison terms in federal juvenile facilities, reported to UNODC that they had been detained because their names were on a wanted list or because somebody in their community had denounced them.[258] This would prevent them from traveling to their home areas to access civil documentation for themselves and any dependents.

Moreover, the Iraqi antiterrorism law penalises severely “anyone who harbours a terrorist”, which has been widely interpreted to include spouses of armed group members. This has led to families being reportedly included in security lists.[259] Iraqi authorities have also collected personal data in Al-Hawl camp in Syria, gathering (allegedly manually) information on Iraqi nationals, including children.[260]

Biometric data management is part of Iraq´s counterterrorism strategy. In 2022 the U.S. Department of State reported that Iraq’s Ministry of Interior had shared biometric data with the U.S. and other partners and held discussions with INTERPOL on data use.[261] But Iraq reportedly lacks capacity to systematically update data systems,[262] reportedly prompting the UN Office of Counterterrorism to consider providing technical support to Iraqi security agencies on screening and data management, to have a uniform consolidated security listing system.[263]

At the same time, as part of its “global war on terror” and pursuit of "identity dominance",[264] the U.S. military in Iraq collected biometric data from thousands of Iraqis, including many never accused of any wrongdoing.[265] The initial U.S. database was set up to capture information on detainees. So, to the extent that detainees were aged under 18 it can be assumed their biometric data was collected.[266] Data collection was then extended to other parts

---

[256] *Global Study on Children Deprived of their Liberty*, July 2019. https://www.ohchr.org/en/treaty-bodies/crc/united-nations-global-study-children-deprived-liberty

[257] *Iraq: The condemned: Women and children isolated, trapped and exploited in Iraq*, Amnesty International, 16 April 2018.

[258] *Targeted by Terrorists: Child Recruitment, Exploitation and Reintegration in Indonesia, Iraq and Nigeria. Strive Juvenile Preventing and Responding to Violence against Children by Terrorist and Violent Extremist Groups*, UNODC.

[259] Interview with Iraqi lawyer. Iraq’s Anti-Terrorism Law No. 13 of 2005, Art. 4.2: “Anyone who intentionally conceals a terrorist act or harbors a terrorist for the purpose of concealment shall be punished by life imprisonment”.

[260] Interview with Iraqi lawyer.

[261] *U.S. Department of State Country Reports on Terrorism 2022;* https://www.biometricupdate.com/202504/thales-helping-iraq-build-biometric-data-center-integrate-id-and-forensic-systems

[262] Interview with Iraqi lawyer.

[263] Interview with confidential source.

[264] The term was coined by John D. Woodward, former director of the U.S. Department of Defense's Biometrics Management Office. He argued that establishing “identity dominance” through a comprehensive Automated Biometric Identification System (ABIS) would “enable the U.S. military to identify friend or foe to keep America safer”. See “Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism” by John D. Woodward in *Military Review*, September-October 2005 at https://www.rand.org/pubs/reprints/RP1194.html.

[265] In 2007, human rights organizations estimated that the U.S. database of biometric information collected in Iraq contained approximately 750,000 records, including fingerprints, photographs, and iris scans. See “Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?” by Krisztina Huszti-Orban and Fionnuala Ní Aoláin, Human Rights Center, University of Minnesota, 2020, p. 7; “Biometric Data Flows and Unintended Consequences of Counterterrorism” by Katja Lindsokov Jacobsen in *International Review of the Red Cross*, no. 916–917 (2022), pp. 619–52.

[266] Discussion with Privacy International.

.

of the population. For instance, U.S. forces required all 'military-aged male' residents to obtain biometric ID cards before being permitted to reenter Fallujah, following the U.S. recapture of the city in late 2004.[267]

Later, using mobile scanners, U.S. forces reportedly gathered fingerprints, eye scans, and other personal data at checkpoints, workplaces, the sites of attacks, and in door-to-door operations.[268] This included biographic and sensitive information such as religious affiliation. In 2007, NGOs raised concerns with the Pentagon about serious risks, including potential reprisals and killings if the database were misused or exploited by future regimes.[269] Adolescent boys, as explained below in the case of Afghanistan, are often viewed as military-aged males.

The U.S. reportedly still retains biometric data on millions of Iraqis (approximately 3 million),[270] and the biometric database ABIS[271] reportedly continues to be used as a resource for U.S. counter-terrorism activities. For instance, U.S. databases connected to ABIS allow the U.S. Department of Homeland Security to block entry to the U.S. to travelers based on biometric data gathered in Afghanistan or Iraq. [272]

All the above practices raise concerns that child detainees and other children, especially adolescent boys considered military aged males and those presumed associated with armed groups through family ties, may be included in security databases, with their data shared and retained indefinitely.

Afghanistan

In Afghanistan, the U.S. military engaged in extensive biometric data collection for security purposes, including from boys deemed military age males.[273] A U.S. army manual on biometric procedures explicitly instructed coalition forces to collect biometric data from "military age males" - with facial photos, iris scans, and fingerprints.[274] Under the assumption that any local individual could pose a future threat, U.S. officials promoted widespread biometric enrollment, advising to incorporate this process into routine activities such as traffic stops, community engagement, at checkpoints, and daily patrols.[275] According to *The Economist* (2012), in volatile regions, "fighting-age males" were thus routinely subjected to iris and fingerprint scans, with patrols at times ordering all men in a village to line up for screening.[276]

[267] *Biometrics and Counter-Terrorism Case study of Iraq and Afghanistan* by Privacy International, May 2021.
[268] Iraqi Biometric Identification System, Electronic Privacy Information Center, https://epic.org/iraqi-biometric-identification-system/
[269] Letter sent in 2007 to U.S. Secretary of Defense by Privacy International, EPIC and Human Rights Watch. See https://epic.org/wp-content/uploads/privacy/biometrics/epic_iraq_dtbs.pdfo
[270] https://www.reuters.com/article/technology/feature-why-does-the-us-still-retain-the-biometrics-of-millions-of-iraqis-idUSL8N35F028/
[271] Automated Biometric Identification System (ABIS) implemented in 2004 by the U.S. Department of Defense to collect biometric data of all its detainees and to track and identify national security threats.
[272] *Biometrics and Counter-Terrorism Case study of Iraq and Afghanistan* by Privacy International, May 2021.
[273] https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan; *Biometrics and Counter-Terrorism, Case study of Iraq and Afghanistan* by Privacy International, May 2021.
[274] *Commander's Guide to Biometrics in Afghanistan, Handbook No. 11-25*, Apr 11, p. 31. The Military-Age Male (MAM) term "is applied to all boys and men, including civilians, who are aged sixteen years and older. The Military-Aged Male category is not synonymous with 'combatant,' but marks boys and men for differentiated treatment in conflict zones, to the point where male bodies are used as a shorthand for 'combatant' when assessing the collateral damage count" for drone strikes. See *Military-Age Males in U.S Counterinsurgency and Drone Warfare* by Sarah Shoker, April 2018. See also "The Necropolitics of Drones" by Jamie Allinson in *International Political Sociology* (2015) 9, 113–127; "From a View to a Kill to Drones and Late Modern War" by Derek Gregory in *Theory Culture Society* 2011 28: 188; https://aoav.org.uk/2019/military-age-males-in-us-drone-strikes/; https://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html; https://www.theguardian.com/world/2012/dec/07/us-military-targeting-strategy-afghanistan.
[275] *Biometrics and Counter-Terrorism, Case study of Iraq and Afghanistan* by Privacy International, May 2021.
[276] https://www.economist.com/asia/2012/07/07/the-eyes-have-it

.

No official U.S. army definition of "military age males" appears to exist, but reports suggest it includes males from age 16—and possibly younger—based on subjective assessments, such as appearance, even remote discretionary determinations by drones or snipers.[277]

The biometric data massively collected under coercive conditions or likely without free and informed consent, was reportedly stored in the Department of Defense's (DoD) Automated Biometric Identification System (ABIS) and cross-referenced with watchlists to target and detain individuals perceived as threats to Afghan and coalition forces.[278] Following the Taliban's takeover in 2021, reports indicate they used U.S. biometric technology (specifically, Handheld Interagency Identity Detection Equipment) to identify and pursue Afghans who had worked with the international coalition.[279]

Somalia

In 2022, the UN reported that Al-Shabaab, a terrorist-designated armed group, had recruited and used 2,259 children (2,181 boys, 78 girls).[280] In 2016 a UN estimate suggested that over half of Al-Shabaab's members were children, some as young as 9. At the time, Al-Shabaab had increasingly targeted children under 15, whom they considered as easier to manipulate.[281] Children have been used as spies,[282] to use explosive devices, and in support roles, such as carrying ammunition or performing domestic chores.[283] Mass abductions of children - mainly boys aged 9–16 - have been one of the group´s main recruitment tactic, girls being also abducted and forcibly married to fighters.[284]

Upon exiting the armed group, defectors are referred by the Somali military to the National Intelligence Security Agency (NISA) for screening and risk assessment. Those individuals considered "low risk" enter a UN-supported DDR programme, and those considered "high risk" are referred to prosecution services.[285] The parameters to be considered high risk though are not clearly stated. NISA´s broad and ill-defined powers have raised serious concerns, including allegations of secret detentions and torture, as noted by the UN Human Rights Committee.[286]

Overall, the stated purpose of "screening" is to determine the role of the individuals within the armed group and to assess their level of risk to decide whether they should be brought to justice for potential prosecution. From a human rights perspective though, no one can be referred for prosecution for a crime they might commit in the future.[287]

---

[277] Though the Military-Age Male (MAM) category references the draft into the army, "the term is applied to all boys and men, including civilians, who are aged sixteen years and older. U.S foreign policy marked boys and men as risky subjects who were more likely to be involved in political violence. Consequently, Military-Age Males technically kept their civilian status, but were highlighted as a risk factor, which enabled conditions for monitoring and profiling. This bureaucratic decision 'made sense' precisely because of historical intellectual labor that sustained the connection between masculinity and political violence. The act of surveillance allowed the United States to maintain a commitment to its legal agreements while simultaneously placing civilian boys and men at greater risk for violent targeting", in *Military-Age Males in U.S Counterinsurgency and Drone Warfare* by Sarah Shoker, April 2018.

[278] "Face Value: Precaution versus Privacy in Armed Conflict " by Leah West in *The Rights to Privacy and Data Protection in Times of Armed Conflict*, Russell Buchan and Asaf Lubin (Eds.).

[279] "Biometric data flows and unintended consequences of counterterrorism" by Katja Lindskov Jacobsen in *International Review of the Red Cross* (2021), 103 (916-917), 619–652.

[280] *Secretary-General Annual Report on Children and Armed Conflict 2022*.

[281] *Secretary-General Annual Report on Children and Armed Conflict 2016*, para. 20.

[282] Former UN worker in Somalia.

[283] *Secretary-General Annual Report on Children and Armed Conflict 2016.*

[284] *Secretary-General Annual Report on Children and Armed Conflict 2022*.

[285] Ministry of Internal Security – Defector Rehabilitation Program "National programme policies and procedures", 1 July 2017.

[286] Human Rights Committee Concluding observations on the initial report of Somalia, 6 May 2024, CCPR/C/SOM/CO/1, para. 25.

[287] Interview with UN worker.

.

Child protection actors have advocated against referring children to NISA for screening and categorization by security services.[288] In 2014, Somalia signed with the UN in-country Standard Operating Procedures (SOPs) which mandate that children follow a separate pathway from adult defectors.[289] According to the SOP, children must be handed over within 72 hours to civilian child protection actors to benefit from interim care and reintegration support.[290] The SOP establish that children may be identified by the military but shall not be interrogated for intelligence purposes. Yet, implementation of the SOP is reportedly inconsistent: children are often not transferred within the agreed time because of logistical or security reasons,[291] and "children are sometimes left in limbo in intelligence facilities, prison or in adult rehabilitation camps for long periods."[292]

Despite the SOP, sources report that most boys exiting Al-Shabaab pass through NISA and undergo NISA-led screening and profiling.[293] Yet, because this is done without the presence of international or humanitarian actors, details of what data is collected, how it is stored, used or shared, remain opaque.[294] Allegedly, the Ministry of Internal Security profiles children post-screening—e.g., as spies or combatants—before transferring them to civilian agencies. "Low risk" status reportedly typically applies to children without military training, and the stated purpose of such profiling is to assess individual needs.[295] After reintegration though, reportedly security forces sometimes use children's data to arrest them or recruit them into NISA to identify former Al-Shabaab peers.[296]

A major challenge in Somalia is the lack of widespread birth registration, which makes it difficult to verify individuals' ages.[297] As a result, adolescents may be mistakenly classified as adults and placed into the adult DDR process, which means they would miss out on the specialized care and reintegration support designed specifically for children leaving armed groups.

Regarding biometric data, the Somali government has reportedly refused to collect it from defectors, citing concerns that leaks or data sharing could lead to travel bans to western countries, other restrictions, and stigmatization. Officials emphasized that defectors are, above all, "daughters and sons of Somalia."[298] Some sources also suggest Al-Shabaab leaders conditioned demobilization on the absence of biometric data collection. So, instead, data on low-risk defectors is reportedly collected manually and recorded in Excel files, without fingerprinting; while data on high-risk individuals is held by NISA, with no public access.[299]

Simultaneously, biometric data is being widely collected in Somalia for humanitarian and border control purposes. The IOM's MIDAS programme, active in Somalia,[300] collects and processes traveler information, aggregates and exchanges migration data, and helps identify security threats,[301] which illustrates how migration, humanitarian,

---

[288] Interviews with researcher and former humanitarian worker in Somalia.
[289] https://childrenandarmedconflict.un.org/2019/10/somalia-increased-measures-to-protect-children-needed-as-grave-violations-against-boys-and-girls-remain-high/; https://unsom.unmissions.org/sites/default/files/sg_report_on_somalia_11_august_2020.pdf
[290] Interview with humanitarian worker in Somalia.
[291] *Ibid* and interview with Disarmament, Demobilization and Reintegration (DDR) section of the UN Assistance Mission in Somalia (UNSOM).
[292] *Somalia: Defection, desertion and disengagement from Al-Shabaab*, European Union Agency for Asylum (EUAA), 2023.
[293] Interviews with humanitarian workers in Somalia.
[294] Interviews with UN worker, and humanitarian worker in Somalia.
[295] Interview with humanitarian worker in Somalia.
[296] Interview with protection worker in Somalia.
[297] Interviews with migration researcher, protection worker, and NGO worker in Somalia.
[298] Discussion with DDR section from UNSOM.
[299] Interview with four humanitarian workers.
[300] The personal data collection programme MIDAS led by IOM captures fingerprints and facial images at border points in at least 16 African countries. https://www.iom.int/sites/g/files/tmzbdl2616/files/documents/midas-brochure18-v7-en_digitall.pdf. It is installed in Somalia's entry points. "Biometric data flows and unintended consequences of counterterrorism" by Katja Lindskov Jacobsen in *International Review of the Red Cross* (2021), 103 (916-917), 619–652.
[301] *Biometrics and Counter-terrorism, Case study of Somalia* by Keren Weitzberg, Privacy International, May 2021.

.

and counterterrorism data may intersect. This raises concerns over potential "risks of data flows between humanitarian and corporate actors, (and) between humanitarian and counterterrorism actors" in Somalia.[302]

Even though Somalia has passed a Data Protection Act, implementation remains weak.[303] Citizens have hence limited legal recourse if their data is misused or if they are erroneously listed or wrongly identified on security watchlists.[304]

Lake Chad Basin

The armed group known as Boko Haram, designated a terrorist group by the UN, has operated since 2009 in the Lake Chad Basin region— comprised of Cameroon, Chad, Nigeria, and Niger. The armed group has employed brutal practices including mass abductions, forced recruitment of children, and the coerced marriage of girls to fighters.[305] In line with a regional strategy on the "Screening, Prosecution, Rehabilitation and Reintegration of Boko Haram Associated Persons", each country in the Lake Chad Basin has adopted measures to deal with persons formerly associated with the armed group, including children.[306]

In **Nigeria**, early counterinsurgency operations in 2016 resulted in the military encountering children in Boko Haram strongholds and relocating them to IDP sites, which functioned as *de facto* internment camps in military facilities. Despite being labeled as ´victims´, children deemed associated with Boko Haram were also seen as security risks and were screened by the Office of the National Security Adviser, to separate alleged 'combatants' from 'non-combatants'. The process was reportedly arbitrary—children from Boko Haram-controlled areas like the Sambisa Forest could be presumed affiliated. Child protection actors had no access to those children classified as combatants, some of whom were interrogated and subject to administrative military detention.[307]

In 2022, the UN reported the detention of 275 children (260 boys, 15 girls), aged between 10 and 17, for actual or alleged association with armed groups. Most were released from Giwa military barracks and Maiduguri Maximum Security Prison in Northeastern Nigeria. During detention, children were interviewed by the Department of State Services to assess their level of involvement with armed groups.[308]

Cooperation by the Nigerian security sector with child protection actors evolved positively, and in 2022 the Government of Nigeria signed a handover protocol mandating the rapid transfer of children allegedly associated with armed groups to civilian child protection actors for reintegration support. Now the Borno State Ministry of Women Affairs and Social Development receives the children for transitional care at the Bulumkutu rehabilitation center in Maiduguri.[309] Those children leaving the armed group together with their families are received in Hajj

---

[302] Jacobsen *supra*.

[303] Interviews with two humanitarian workers in Somalia.

[304] *Biometrics and Counter-terrorism, Case study of Somalia* by Keren Weitzberg, Privacy International, May 2021.

[305] *"We dried our tears" Addressing the toll on children of Northeast Nigeria's conflict*, Amnesty International 2020; *Violations and abuses committed by Boko Haram and the impact on human rights in the countries affected, Report of the United Nations High Commissioner for Human Rights*. A/HR/C/30/67, 9 December 2015; *"Those Terrible Weeks in Their Camp", Boko Haram Violence against Women and Girls in Northeast Nigeria*, Human Rights Watch, October 2014.

[306] Following Security Council resolution 2349, the African Union Commission, the Lake Chad Basin Commission, and international partners promoted a shared, beyond military, approach to stabilization in the region with resulted in a "Regional Strategy for the Stabilization, Recovery and Resilience of the Boko Haram-affected areas of the Lake Chad Basin Region (RSS)", adopted in 2018. See *The State of Play. Process and Procedures for Screening, Prosecution, Rehabilitation and Reintegration in the Lake Chad Basin Region, Background Study Report*, UNDP, January 2023.

[307] Interviews conducted by the author in 2016 with former UN staff and INGO human rights´ researchers on Nigeria at the time.

[308] *Children and armed conflict in Nigeria, Report of the Secretary-General* S/2022/596, 4 August 2022, para. 26.

[309] *Advancing Holistic and Comprehensive Efforts to Confront Africa's Growing Terrorism Challenge: A Nigerian Case Study on Developing Sustainable Pathways Out of Extremism for Individuals Formerly Associated with Boko Haram and ISWAP,* CCCPA, Cairo, 2022; *Secretary-General Annual Report on Children and Armed Conflict 2022*.

.

camp, which was set up following mass exits from the armed group. Also in 2022, the Nigerian government launched a "Call for Action" led by the Office of the National Security Adviser, which formally acknowledges that children formerly associated with armed groups should be considered and treated primarily as victims.[310]

Regarding personal data, at least two databases reportedly store information on individuals disengaging from armed groups—one for reintegration and one for security purposes.[311] As for children, a child protection information management system (CPIMS+) is co-managed by the Borno state, to facilitate family reunification, rehabilitation and reinsertion support services to the children formerly associated with Boko Haram. On the security side, the Nigerian military initially created individual profiles of children at Giwa barracks prior to their transfer to civilian authorities.[312] Currently, still the military conduct so-called "screening" of children exiting Boko Haram who are usually encountered in remote locations. UNICEF has conducted training and provided guidance to the military not only on the handover protocol but also on this so-called "screening", which includes age verification to separate children from adults existing the armed group.[313] It remains unclear though the full extent of security-led collection of children´s data or its purpose. The complexity of the reintegration pathways—spread across state and federal level as well as governmental and non-governmental actors[314]—may prevent children from fully understanding and describing who exactly collected their data or why.[315]

In **Niger**, persons allegedly associated with armed groups are referred by the armed forces to antiterrorist cells or to one of the antiterrorist antennas located in different regions, which then transfer cases to the Prosecutor's Office. In February 2017 the Government of Niger and the UN system signed a handover protocol for the rapid transfer of children associated with armed groups to civilian authorities. In conformity with the handover protocol, when the individual exiting armed groups is a child, the case goes to a Children's Judge, who orders temporary placement of the child in a transit center and oversees the case until issuing a final judicial decision for the child´s return to his/her family. These cases are filed as "child protection" cases, but if the child is suspected of criminal acts while associated with the armed group, a juvenile justice file can be then opened. Judges reportedly struggled at first to accept that children exiting terrorist groups would be sent to civilian-run transit centers, while those children who committed minor common offences could be detained.[316]

The Niger law prohibits sharing information about children involved in criminal offenses, whether related to terrorism or not. However, in practice, children's data reportedly often circulates widely — exchanged between magistrates and sometimes shared across government bodies, such as the Ministry of Justice and the Ministry of Foreign Affairs, especially when children leave armed groups. There is also reportedly a parallel system run by the military, and children´s data is transferred through the military hierarchy. As well, the Multinational Joint Task Force, integrated by armed forces from Lake Chad Basin countries, reportedly hold their own files on the people they have arrested, presumably including children.[317]

INTERPOL is allegedly informed of all individuals registered by the antiterrorist cell and antennas, the investigation services and in prisons, including children.[318]

---

[310] Discussion with UNODC. See https://www.unodc.org/unodc/en/justice-and-prison-reform/strive/newsroom_nigeria-call-for-action_dec-2022.html

[311] Interviews with two UN workers in Nigeria and the Lake Chad Basin.

[312] Interview with humanitarian worker in Nigeria.

[313] Discussion with UNICEF.

[314] There is no one single point of entry. So, the children may talk to different authorities, as well as with humanitarian workers. Discussion with UN worker.

[315] Interview with researcher on the Lake Chad Basin.

[316] Interview with lawyer from Niger.

[317] *Ibid.*

[318] Interview with lawyer from Niger.

.

In **Cameroon**, a 2018 presidential decree established the National Disarmament, Demobilization and Reintegration Committee (NDDRC) to implement and oversee DDR processes for both the Far-North, and the North-West & South-West regions. In the Far-North, individuals who voluntarily disengage from Boko Haram—including not only former combatants but also people deemed "associated" with the group through various support roles, along with their dependents[319]—are often received first by the military (either the Cameroonian army or its Sector 1 of the regional multinational force[320]). These groups — former combatants, alleged associates and dependents—can all include children.[321] They are then transferred to an NDDRC-run center in Meri, located in the Far North region. Before being transferred to DDR services, they undergo personal data collection by the military, who are so-called "points of first contact" especially in isolated military posts which are closest to Boko Haram´s presence.[322] This initial personal data collection is focused on security rather than identifying socio-economic reintegration needs. Yet, due to the confidential nature of the process, it is unclear what specific data is collected or how it is used by security actors.[323] The data collected by the army is reportedly not sent to the NDDRC. The army keeps its data. The NDDRC, with the support of IOM, collects new data to be used for socio-economic profiling, which is limited to adults.[324]

While some former combatants and associates, including children, have been detained and charged, Cameroon's approach has generally prioritized reintegration over prosecution. Nonetheless, community reinsertion efforts have been slow and underfunded. Even though a handover protocol, for the swift transfer of children allegedly associated with Boko Haram to child protection actors, was developed at the technical level,[325] Cameroon has not yet officially signed the handover protocol. This is reportedly due to ongoing concerns that some of these children may pose security risks.[326]

In Chad, Cameroon and Niger individuals´ criminal records are reportedly kept on paper files; the files may get lost or disappear - while computerised files can be shared in a matter of minutes. In a sense, lack of technology is positive for children associated to armed groups as their data and files may not be kept for very long.[327]

[319] The term "associates" englobes persons including children under 18, with no fighting roles, such as cooks, those married to Boko Haram members, those providing logistical support, and children born of associates. Interview with confidential source.
[320] The Multinational Joint Task Force (MNJTF) is composed by armed forces from Chad, Cameroon, Nigeria, Niger and Benin. In late March 2025, Niger reportedly withdrew from the MNJTF.
[321] Interviews with UN worker, three confidential sources, director of NGO ALDEPA and with Annabelle Bonnefont, Senior Legal Analyst for the Global Center on Cooperative Security.
[322] Interviews with two confidential sources based in Cameroon.
[323] Interviews with UN worker, three confidential sources, and director of NGO ALDEPA.
[324] Interview with UN worker.
[325] https://www.iom.int/news/taking-account-specific-needs-children-national-ddr-process, https://www.iom.int/news/disarmament-and-reintegration-cameroon-has-made-protection-children-context-ddr-priority
[326] Interviews with confidential sources familiar with the DDR process in Cameroon. The highest political endorsement of the protocol is still pending.
[327] Interview with UN worker.

.

Annex II – EU and other regulatory frameworks and guidance

EU and other security agencies´ regulatory frameworks

The European Union Guidelines on children affected by armed conflict recognize children forcibly recruited by armed groups as victims and expressly state that arresting or detaining children because they are perceived as a national security threat or because they have allegedly participated in hostilities, further victimize them.[328] These Guidelines, however, do not address the issue of collection and use of children´s personal on counterterrorism grounds in conflict or post conflict settings.

The EU has strong legal frameworks for data protection. The General Data Protection Regulation (GDPR), applicable in EU countries and the UK,[329] is one of the world's most comprehensive data protection regimes. It outlines core data protection principles, individual rights, and State obligations. The GDPR highlights that children require "specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data" (Recital 38).[330]

Article 6(1)(f) permits data processing when necessary for legitimate interests pursued by the controller or by a third party, unless outweighed by the interests or fundamental rights and freedoms of the data subject—particularly if the data subject is a child. However, this does not apply to data processing by public authorities in the performance of their duties.[331] Nevertheless, data processing for security or law enforcement purposes must still comply with general data protection principles, which apply to children and adults alike, as outlined below.

The EU Law Enforcement Directive (Directive 2016/680) governs the processing of personal data for law enforcement purposes, including the "prevention of threats to public security", and the transfer of such personal data to third countries and international organizations.[332] It mandates that personal data processing be lawful, fair, and transparent; limited to explicit, legitimate purposes laid down by law; and not excessive or retained longer than necessary for the purpose for which they are processed (Art. 26).

The Directive acknowledges children as vulnerable persons who deserve special protection (Recitals 39 and 50), which could be interpreted as equaling data on children to "special categories of data" deserving heightened safeguards. However, these recitals are strong interpretative aids but ultimately non-binding.[333] Further, the

[328] "The best interests of the child is the primary consideration in the implementation of EU action…The forced recruitment of children under the age of 18 and their use in hostilities by both armed forces and armed groups is illegal and one of the worst forms of child labor. Furthermore, the recruitment of children under 15 constitutes a war crime. It places an inhumane burden and long term detrimental consequences on these children, who remain primarily victims and often face stigma and rejection. Arresting and detaining children associated with armed groups, whether because they are perceived as a threat to national security or because they have allegedly participated in hostilities, further victimizes them." See EU Guidelines on Children and Armed Conflict, first published 2008, revised 2024.

[329] The UK GDPR is the same in content as the EU GDPR at the time of Brexit, but with some localized changes and different governance.

[330] See also Recital 58: "…Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand." Article 8 stipulates conditions applicable to the child's consent in relation to information society services.

[331] https://gdpr-info.eu/art-6-gdpr/

[332] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[333] Recitals explain the rationale and contents of the operative provisions of the norm and provide guidance for its interpretation, especially of ambiguous provisions. The Court of Justice of the European Union (CJEU) often resorts to recitals to help clarify the intent and explain the meaning of unclear legal texts. In CJEU case C-755/21 P (paras. 59-61), the Court affirms that recitals are an important interpretive aid, but they do not prevail over operative provisions in case of inconsistency.

.

European Data Protection Supervisor (EDPS) expressly noted that the Directive (in Article 6) requires differentiation between personal data of suspects, convicted persons, victims, and witnesses, but does not treat individuals under 18 years as a separate category of data subjects.[334]

The EUROPOL Regulation includes similar general principles as the above Law Enforcement Directive.[335] It also expressly provides specific safeguards for children´s data:

- Article 30 limits the processing and transfer of children´s personal data to what is strictly necessary and proportionate to prevent or combat crime. The European Data Protection Supervisor (EDPS) has emphasized that assessing necessity and proportionality in such cases involving children´s data is highly contextual and cannot be done *in abstracto.*[336]
- Article 31(5) requires EUROPOL to inform the EDPS if it processes data on persons under 18 for more than five years.
- Article 43 highlights that data processing may risk individuals' rights and freedoms, especially for vulnerable groups like children, and mandates extra protection for data related to victims, witnesses, and children. The Regulation expressly refers to children victims of sexual abuse. It does not clarify though whether such special protections equally apply to children considered suspects.

The EU Schengen Information System (SIS) Regulation in the field of border checks allows the processing of biometric data for reliable identification but mandates it be limited to what is lawful and necessary for the objectives pursued. It explicitly requires that **in cases concerning children, the best interests of the child should be a primary consideration**.[337] The SIS Regulation includes a specific provision protecting children as 'vulnerable' individuals to prevent them from travelling without the necessary authorization - and thus combat child trafficking, as well as protect children at risk of being abducted by their own parents, relatives or guardians.[338] The Regulation is silent though on whether children can be also considered suspects.[339] Under the Regulation, suspects who are the object of an "alert" may be tracked under discreet surveillance without their knowledge.

EURODAC helps EU states to determine responsibility for examining an asylum application by comparing fingerprint datasets. The updated EURODAC Regulation (2024) allows collection and storage of biometric data from children over 6 years of age, and retain the data for up to ten years.[340] Use of data from children under 14 for law enforcement purposes requires additional justification beyond general thresholds, to consider such data necessary

---

[334] *European Data Protection Supervisor report on inspection at EUROPOL, Conducted pursuant to Article 47(2) of Regulation (EC) No. 45/20011 and Article 43(4) of Regulation (EU) No. 2016/794*, 19 December 2018, Case Reference 2018-0067.

[335] EUROPOL Regulation (EU) 2016/794 of 11 May 2016 in Article 28 on General data protection principles states that personal data shall be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed; (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; and (f) processed in a manner that ensures appropriate security of personal data.

[336] *European Data Protection Supervisor report on inspection at EUROPOL, conducted pursuant to Article 47(2) of Regulation (EC) No. 45/20011 and Article 43(4) of Regulation (EU) No. 2016/794*, 19 December 2018, Case Reference 2018-0067.

[337] The SIS Regulation states that it "fully respects the protection of personal data in accordance with Article 8 of the Charter of Fundamental Rights of the European Union while seeking to ensure a safe environment for all persons residing on the territory of the Union and protection of irregular migrants from exploitation and trafficking in human beings. In cases concerning children, the best interests of the child should be a primary consideration." (Art 20 of Regulation (EU) 2018/1861 of the European Parliament and of The Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006).

[338]https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system/alerts-and-data-sis_en. Interview with Niovi Vavoula.

[339] Interview with Niovi Vavoula.

[340] Regulation (EU) 2024/1358 of the European Parliament and of the Council of 14 May 2024, Articles 22 and 23.

.

for the purpose of the prevention, detection or investigation of a terrorist offence or other serious criminal offence which that child is suspected of having committed (Art.14.3).

Other EU framework documents stipulate information exchange between EU databases on asylum and immigration, INTERPOL, and EUROPOL as central to counterterrorism efforts.[341]

INTERPOL manages 19+ databases and retains control over the sharing of certain biometric data.[342] INTERPOL Guidance on Personal Data Processing includes a specific provision on children, stating that when recording data involving children it must be **explicitly inserted the term "minor",** also indicating the age of majority under the respective national law.[343] However, it does not specify any special protections for such data related to "minors". It is also unclear whether this requirement applies only to child victims or also to child suspects, this suggesting it may apply to all children.

It is important to note that the age of majority—and thus the level of protection INTERPOL may apply to a "minor's" personal data—can differ depending on the laws of each country. For example, Somalia sets the age of majority at 15 (as of March 2024),[344] while Iraq distinguishes between "preadolescents" (9–15) and "adolescents" (15–18).[345]

UN counterterrorism guidance on data collection

As above mentioned, UN Security Council resolutions call on States to collect and share personal data, including biometric data, for counterterrorism purposes. UN bodies have issued guidance advocating a human rights-based approach to such personal data collection and use, which includes some references to children's rights. Most of the child related guidance remains quite general though, typically including a broad recommendation to consider children's best interests, or to establish specific safeguards for children, without detail on what such safeguards for children's data would entail. Key examples include:

Madrid Guiding Principles + 2018 Addendum on Foreign Terrorist Fighters, Principle 42:[346] Calls for full respect and promotion of children's rights, "taking into account the **best interests of the child as a primary consideration**". It

[341] EU Council conclusions on future priorities for strengthening the joint counterterrorism efforts of the European Union and its Member States (C/2025/300); https://www.consilium.europa.eu/en/policies/fight-against-terrorism/#information%20exchange;

[342] *Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences*, Counter-Terrorism Committee Executive Directorate (CTED).

[343] INTERPOL'S Rules on the Processing of Data, Article 38 (1): Additional conditions for recording data on persons shall be applicable in the following cases:
(a) data on deceased persons;
(b) data on victims or witnesses;
(c) data on minors;
(d) particularly sensitive data.
Article 41: Additional conditions for recording data on minors
(1) The additional indication "MINOR" must be inserted whenever the person was a minor at the time of the event or act which is being recorded. The age at which a minor attains majority shall be determined in the light of the national laws of the National Central Bureau or the national entity that recorded the data or, in the case of an international entity, in the light of the applicable rules.
(2) In this case, the National Central Bureau, national entity or international entity which records the data shall specify any particular conditions imposed by applicable national laws.

[344]https://www.pila.ie/resources/bulletin/2024/04/10/somalian-constitutional-change-lowers-the-age-of-maturity-leaving-children-potentially-vulnerable/

[345] https://www.unicef-irc.org/portfolios/documents/396_iraq.htm

[346] *Security Council Guiding Principles on Foreign Terrorist Fighters: The 2015 Madrid Guiding Principles + 2018 Addendum*, Guiding principle 42.

.

recommends to "consider…(vi) developing and implementing **specific frameworks and safeguards in matters concerning data of children** and victims of terrorism, in particular victims of sexual violence committed with terrorist intent, in situations where they may be placed on databases…"

Security Council Counter-Terrorism Committee Executive Directorate (CTED) Battlefield Evidence Guidance: Urges specialized training on handling women and children and their possible involvement in a judicial process, recognizing children as potential victims of terrorism. Recommends **special safeguards** and legal protections in line with States´ international obligations to respect and promote the rights of the child, **taking into account the best interests of the child as a primary consideration.**[347]

UN Handbook on Children Affected by the Foreign-Fighter Phenomenon (UN-OCT and UNICEF): Offers detailed guidance in a final chapter specifically dedicated to children's personal data, rooted in international human rights law.[348]

[347] *Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offence*, Counter-Terrorism Committee Executive Directorate (CTED).
[348] *Handbook, Children affected by the foreign-fighter phenomenon: Ensuring a child rights-based approach,* United Nations Office on Counterterrorism, UN Counterterrorism Center, Chapter 8.